

**SECTOR Service Level Agreement  
Between  
Winthrop Marshal's Office  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Winthrop Marshal's Office (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
- 5. Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
- 6. Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
- 7. Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
- 8. WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
- 9. Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.


**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

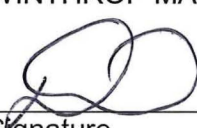
**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

WINTHROP MARSHAL'S OFFICE

  
Signature  
Date

  
Signature  
Date

13 JUL 10

Jeff Hugsdale, Contracts  
Printed Name and Title  
MANAGER

MARSHAL DAVID DAULSTROM 901  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

Technical issues and change requests:

Marshal David Dahlstrom

(509) 996-2160

cell: (509) 341-4125

[marshal@townofwinthrop.com](mailto:marshal@townofwinthrop.com)

Service Level Agreement issues:

Same as above



WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Winthrop Police Department is hereby amended as follows:


- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.

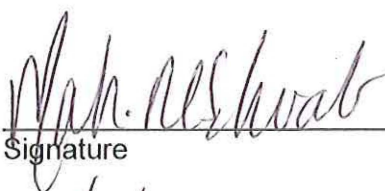
All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

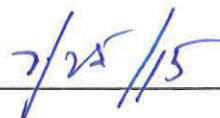
STATE OF WASHINGTON  
WASHINGTON STATE PATROL

WINTHROP POLICE DEPARTMENT

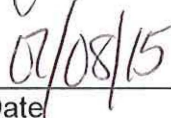
  
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_  
Signature

Date

  
\_\_\_\_\_  
Date

Date

  
\_\_\_\_\_  
Date

**SECTOR Service Level Agreement  
Between  
Lake Forest Park Police Department  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Lake Forest Park Police Department (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
- c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
- d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
- e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
- f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
- g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
- 5. Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
- 6. Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
- 7. Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
- 8. WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
- 9. Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.


**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.


**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

LAKE FOREST PARK POLICE  
DEPARTMENT

  
Signature  
Date

  
Signature  
Date

  
Printed Name and Title  
Manager

  
Printed Name and Title  
Chief of Police

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.



## **APPENDIX C**

### **Project Contacts**

1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

2. For the Agency:

Technical issues and change requests:

Rhonda Siner

(206) 957-2898

[rsiner@ci.lake-forest-park.wa.us](mailto:rsiner@ci.lake-forest-park.wa.us)

Service Level Agreement issues:

Sergeant Jason Becker

(206) 364-8216

[jbecker@ci.lake-forest-park.wa.us](mailto:jbecker@ci.lake-forest-park.wa.us)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Lake Forest Park Police Department is hereby amended as follows:

- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

LAKE FOREST PARK  
POLICE DEPARTMENT

*for*  
  
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_  
Signature

*7/9/15*  
\_\_\_\_\_  
Date

*7-9-15*  
\_\_\_\_\_  
Date

**SECTOR Service Level Agreement  
Between  
Auburn Police Department  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Auburn Police Department (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
- 5. Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
- 6. Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
- 7. Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
- 8. WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
- 9. Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

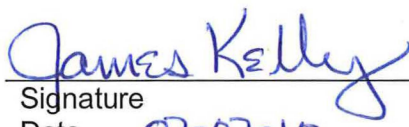
**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

AUBURN POLICE DEPARTMENT

  
Signature  
Date

  
Signature  
Date

  
Printed Name and Title

  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.



## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

Technical issues and change requests:

Brian Garbarino, Network Engineer

(253) 804-5025

[bgarbarino@auburnwa.gov](mailto:bgarbarino@auburnwa.gov)

Service Level Agreement issues:

Assistant Chief Bob Karnofski

(253) 804-3115

[bkarnofski@auburnwa.gov](mailto:bkarnofski@auburnwa.gov)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Auburn Police Department is hereby amended as follows:

- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.


All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

AUBURN POLICE DEPARTMENT

*for*   
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date *7/22/15*

\_\_\_\_\_  
Date *7/13/15*

**SECTOR Service Level Agreement  
Between  
Tacoma Police Department  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Tacoma Police Department (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
- 5. Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
- 6. Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
- 7. Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
- 8. WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
- 9. Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.


**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

TACOMA POLICE DEPARTMENT

  
\_\_\_\_\_  
Signature  
Date

  
\_\_\_\_\_  
Signature  
Date

  
\_\_\_\_\_  
Printed Name and Title

  
\_\_\_\_\_  
DONALD RAMSDALL, POLICE CHIEF  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

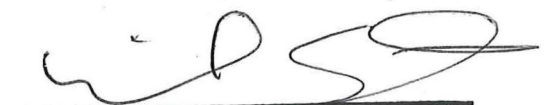
Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

**APPROVED AS TO FORM:**

  
\_\_\_\_\_  
Michael J. Smith  
Police Legal Advisor  
Assistant City Attorney

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in



the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

Technical issues and change requests:

Clayton Krauss

(253) 591-5073

[ckrauss@ci.tacoma.wa.us](mailto:ckrauss@ci.tacoma.wa.us)

Service Level Agreement issues:

Sergeant Frank Richmond

(253) 591-5347

[frichmon@cityoftacoma.org](mailto:frichmon@cityoftacoma.org)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Tacoma Police Department is hereby amended as follows:


- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.


All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

TACOMA POLICE DEPARTMENT


*for*   
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_  
Signature

*7-22-15*  
\_\_\_\_\_  
Date

*7/14/2015*  
\_\_\_\_\_  
Date

**APPROVED AS TO FORM:**

   
\_\_\_\_\_  
Michael J. Smith  
Police Legal Advisor  
Assistant City Attorney

**SECTOR Service Level Agreement  
Between  
Shoreline Police Department  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Shoreline Police Department (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
- c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
- d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
- e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
- f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
- g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
- 5. Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
- 6. Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
- 7. Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
- 8. WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
- 9. Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

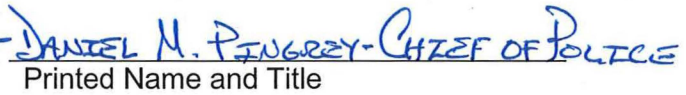
STATE OF WASHINGTON  
WASHINGTON STATE PATROL

SHORELINE POLICE DEPARTMENT

  
Signature  
Date

  
Signature  
Date

  
Printed Name and Title

  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts



## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

Technical issues and change requests:

Sergeant Bruce Bartlett

(206) 801-2756

[bruce.bartlett@kingcounty.gov](mailto:bruce.bartlett@kingcounty.gov)

Service Level Agreement issues:

Chief Daniel Pingrey

(206) 801-2710

[Daniel.pingrey@kingcounty.gov](mailto:Daniel.pingrey@kingcounty.gov)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Shoreline Police Department is hereby amended as follows:


- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.


All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

SHORELINE POLICE DEPARTMENT

*for*   
\_\_\_\_\_  
John R. Batiste, Chief  
  
*8/12/15*  
\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Signature SHAWN LEDFORD, CHIEF  
  
*8/7/15*  
\_\_\_\_\_  
Date

**SECTOR Service Level Agreement  
Between  
Yakima County Prosecuting Attorney's Office  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Yakima County Prosecuting Attorney's Office (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
- 5. Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
- 6. Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
- 7. Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
- 8. WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
- 9. Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.



**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

  
Signature  
Date 8/12/10

Jeff Husdahl, Contracts Manager  
Printed Name and Title

YAKIMA COUNTY PROSECUTING  
ATTORNEY'S OFFICE

  
Signature  
Date 8/4/10

James V. Haberman, Prosecuting Attorney  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

Technical issues and change requests:

Kerrie Maybee

[Kerrie.maybee@co.yakima.wa.us](mailto:Kerrie.maybee@co.yakima.wa.us)

Service Level Agreement issues:

Susan Arb

[Susan.arb@co.yakima.wa.us](mailto:Susan.arb@co.yakima.wa.us)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Yakima County Prosecuting Attorney is hereby amended as follows:

- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

YAKIMA COUNTY PROSECUTING  
ATTORNEY



*for* \_\_\_\_\_  
John R. Batiste, Chief

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

*2/9/15*

\_\_\_\_\_  
Date

*July 6, 2015*

**SECTOR Service Level Agreement  
Between  
Longview City Attorney  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Longview City Attorney (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.



- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
- 5. Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
- 6. Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
- 7. Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
- 8. WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
- 9. Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

LONGVIEW CITY ATTORNEY

*[Signature]*      8/12/10  
Signature      Date

*[Signature]*  
Signature  
7/28/10  
Date

*Jeff Hagedahl, Contracts*  
Printed Name and Title      MANAGER

*Marilyn K. Nitteberg-Haan*  
Printed Name and Title      City Attorney

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management; the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

Technical issues and change requests:

Judy Jones

[Judy.jones@ci.longview.wa.us](mailto:Judy.jones@ci.longview.wa.us)

Service Level Agreement issues:

Marilyn Haan

[Marilyn.haan@ci.longview.wa.us](mailto:Marilyn.haan@ci.longview.wa.us)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Longview City Attorney is hereby amended as follows:

- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.

All other terms and conditions of this Contract remain in full force and effect.

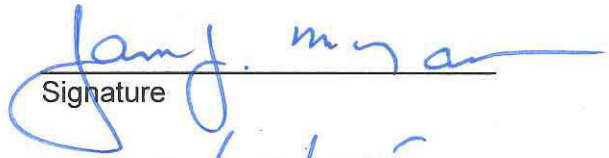
THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

LONGVIEW CITY ATTORNEY

*for*   
John R. Batiste, Chief

7-8-15  
Date

  
Signature

6/29/15  
Date

**SECTOR Service Level Agreement  
Between  
Everett Police Department  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Everett Police Department (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;



- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

EVERETT POLICE DEPARTMENT

  
Signature  
Date

7/2/10

  
Signature  
Date

8-31-10

Jeff Houghland, Contracts Manager  
Printed Name and Title

Jim Schindler, Chief of Police  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (Pierce County v. Guillen, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

#### **1. For WSP:**

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### **2. For the Agency:**

Technical issues and change requests:

Jerry Diedrichs, IT Manager

(425) 257-8683

[jdiedrichs@ci.everett.wa.us](mailto:jdiedrichs@ci.everett.wa.us)

Service Level Agreement issues:

Captain Dan Templeman

(425) 257-8493

[dtempleman@ci.everett.wa.us](mailto:dtempleman@ci.everett.wa.us)

CITY OF EVERETT

By Ray Stephanson  
Ray Stephanson, Mayor

Dated: 12-8-2010

ATTEST:  
By Sharon Marks  
Sharon Marks, City Clerk

Dated: 12/8/10

APPROVED AS TO FORM:

By James A. He  
City Attorney

Dated: 12/2/10



WSP Contract No. C110278GSC  
Amendment 1

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Everett Police Department is hereby amended as follows:

- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

EVERETT POLICE DEPARTMENT

*per*   
\_\_\_\_\_  
John R. Batiste, Chief

 #291  
\_\_\_\_\_  
Signature

*8/3/15*  
\_\_\_\_\_  
Date

*7-8-15*  
\_\_\_\_\_  
Date

AGREED:

CITY OF EVERETT, WASHINGTON

By:

Ray Stephanson

Ray Stephanson, Mayor

Date:

7/30/2015

ATTEST:

Sharon Fuller

Sharon Fuller, City Clerk

Date:

7/30/2015

APPROVED AS TO FORM:

James D. Iles

James D. Iles, City Attorney

Date:

7/29/15

**SECTOR Service Level Agreement  
Between  
Kittitas County Prosecuting Attorney's Office  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Kittitas County Prosecuting Attorney's Office (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
- 5. Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
- 6. Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
- 7. Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
- 8. WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
- 9. Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

  
Signature  
Date

*Jeff Hurdahl, Contracts Manager*  
Printed Name and Title

KITTITAS COUNTY PROSECUTING  
ATTORNEY'S OFFICE

  
Signature  
Date

*Greg Zempel Prosecutor*  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.



## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

Technical issues and change requests:

Duke Senter, IT Administrator

(509) 962-7510

[Duke.senter@co.kittitas.wa.us](mailto:Duke.senter@co.kittitas.wa.us)

Service Level Agreement issues:

Gregory Zempel, County Prosecutor

(509) 962-7520

[Greg.zempel@co.kittitas.wa.us](mailto:Greg.zempel@co.kittitas.wa.us)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Kittitas County Prosecuting Attorney's Office is hereby amended as follows:

- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

KITTITAS COUNTY PROSECUTING  
ATTORNEY'S OFFICE

*John R. Batiste*  
\_\_\_\_\_  
John R. Batiste, Chief

*[Signature]*  
\_\_\_\_\_  
Signature

*7/2/15*  
\_\_\_\_\_  
Date

*06-29-15*  
\_\_\_\_\_  
Date

 **MAILED**  
*7/8/2015*

**SECTOR Service Level Agreement  
Between  
City of Lacey  
And  
Washington State Patrol**

- 1. Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Police Department of the City of Lacey (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
- 2. Description of SECTOR.** SECTOR has three primary parts:

  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
- 3. Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:

  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
- 5. Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
- 6. Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
- 7. Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
- 8. WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
- 9. Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.


**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

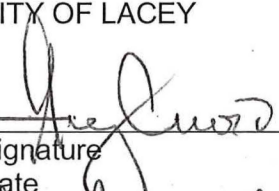
**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.


The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

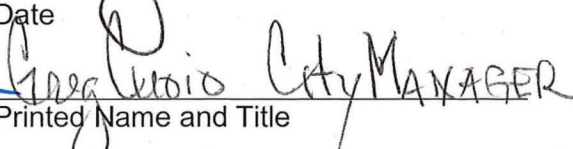
STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF LACEY

  
\_\_\_\_\_  
Signature  
Date

  
\_\_\_\_\_  
Signature  
Date

  
\_\_\_\_\_  
Printed Name and Title

  
\_\_\_\_\_  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in



the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

##### Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

##### Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

##### Technical issues and change requests:

Cindy Zielinski, Information Services Manger

(360) 438-2626

[Czielinski@ci.lacey.wa.us](mailto:Czielinski@ci.lacey.wa.us)

##### Service Level Agreement issues:

Greg Cuoio, City Manager

(360) 491-3214

[Gcuoio@ci.lacey.wa.us](mailto:Gcuoio@ci.lacey.wa.us)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Lacey Police Department is hereby amended as follows:


- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

LACEY POLICE DEPARTMENT

  
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_  
Signature

  
\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Date

**SECTOR Service Level Agreement  
Between  
Mukilteo Police Department  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Mukilteo Police Department (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
- c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
- d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
- e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
- f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
- g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

MUKILTEO POLICE DEPARTMENT

Signature

Date

Signature

Date

Jeff Hagedahl, Contracts Manager  
Printed Name and Title

Dir. Hanson City Administrator  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts



## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

Technical issues and change requests:

David Varga, Director of IT

(425) 263-8000, ext 8037

[dvarga@ci.mukilteo.wa.us](mailto:dvarga@ci.mukilteo.wa.us)

Service Level Agreement issues:

Charles Macklin, Commander

(425) 263-8100, ext 8102

[cmacklin@ci.mukilteo.wa.us](mailto:cmacklin@ci.mukilteo.wa.us)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Mukilteo Police Department is hereby amended as follows:

- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.


All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

MUKILTEO POLICE DEPARTMENT

*for*   
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_  
Signature *REX D. CALDWELL, Chief*

*7-2-15*  
\_\_\_\_\_  
Date

*7-2-15*  
\_\_\_\_\_  
Date

**SECTOR Service Level Agreement  
Between  
Grays Harbor County Prosecuting Attorney's Office  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Grays Harbor County Prosecuting Attorney's Office (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
- 5. Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
- 6. Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
- 7. Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
- 8. WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
- 9. Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.



**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

Signature

Date

*Jeff Haddad* 11/3/10

Printed Name and Title

Jeff Haddad, Contracts Manager

GRAYS HARBOR COUNTY  
PROSECUTING ATTORNEY'S OFFICE

Signature

Date

*H. Steward Menefee* 11/2/10

Printed Name and Title

H. Steward Menefee, Prosecutor

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

Technical issues and change requests:

Dale Gowan, Central Services

(360) 249-4144x454

[dgowan@co.grays-harbor.wa.us](mailto:dgowan@co.grays-harbor.wa.us)

Service Level Agreement issues:

H. Steward Menefee, County Prosecuting Attorney

(360) 249-3951x109

[smenefee@co.grays-harbor.wa.us](mailto:smenefee@co.grays-harbor.wa.us)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Grays Harbor County Prosecuting Attorney's Office is hereby amended as follows:

- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.


All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

GRAYS HARBOR COUNTY  
PROSECUTING ATTORNEY'S OFFICE

  
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_  
Signature

Date

  
\_\_\_\_\_  
Date

Date

  
\_\_\_\_\_  
Date

**SECTOR Service Level Agreement  
Between  
City of Kent  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Law Department for the City of Kent (acting as prosecutor in the Kent Municipal Court under Section 2.20 of the Kent Municipal Code), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;
    - Update required Agency processes with the parameters of SECTOR.

- Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
  - b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.
  - b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.



- c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
- 5. Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
- 6. Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
- 7. Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
- 8. WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
- 9. Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.
- 10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.

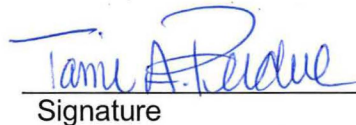
- 11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.
- 12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.
- 13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.
- 14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF KENT

 11/17/10  
Signature Date

 11/10/10  
Signature Date

  
Printed Name and Title

  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

- Appendix A - Statement on Collision Records Data
- Appendix B - SECTOR Governance Committee Training Policies
- Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

Technical issues and change requests:

Kim Clements, Senior System Analyst

(253) 856-4623

[kclements@ci.kent.wa.us](mailto:kclements@ci.kent.wa.us)

Service Level Agreement issues:

Tami Perdue, Chief Prosecuting Attorney

(253) 856-5776

[tperdue@ci.kent.wa.us](mailto:tperdue@ci.kent.wa.us)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the City of Kent is hereby amended as follows:

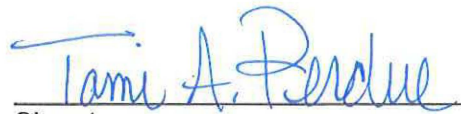
- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF KENT



*for*  
\_\_\_\_\_  
John R. Batiste, Chief

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

*7/22/15*

\_\_\_\_\_  
Date

*7-15-2015*

**SECTOR Service Level Agreement  
Between  
Cosmopolis Police Department  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Cosmopolis Police Department (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;



- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
- c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
- d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
- e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
- f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
- g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

COSMOPOLIS POLICE DEPARTMENT

Signature

Date

Signature

Date

Printed Name and Title

Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

Technical issues and change requests:

Casey Stratton, Chief of Police

(360) 532-9237

[cstratton@cosmopolis.us.com](mailto:cstratton@cosmopolis.us.com)

Service Level Agreement issues:

Heath Layman, Deputy Chief

(360) 532-9237

[hlayman@cosmopolis.us.com](mailto:hlayman@cosmopolis.us.com)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Cosmopolis Police Department is hereby amended as follows:



- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.

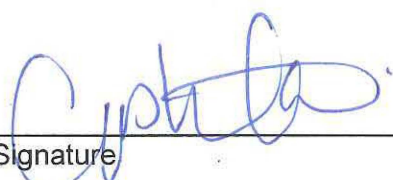
All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

COSMOPOLIS POLICE DEPARTMENT

  
\_\_\_\_\_  
John R. Batiste, Chief  
  
\_\_\_\_\_  
Date 01/30/15

  
\_\_\_\_\_  
Signature  
\_\_\_\_\_  
Date 01/29/2015



**SECTOR Service Level Agreement  
Between  
City of Port Townsend  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Attorney's Office for the City of Port Townsend as defined in Section 2.08.040 of the Port Townsend Municipal Code, referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;
    - Update required Agency processes with the parameters of SECTOR.

- Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
  - b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.
  - b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.

- c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.
10. **Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.


- 11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.
- 12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.
- 13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.
- 14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF PORT TOWNSEND

 12/14/10  
Signature Date

 12-8-10  
Signature Date

  
Printed Name and Title

DAVID TIMMONS CITY MGR  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

Technical issues and change requests:

Mark Peil, IT

(360) 390-5850

[mpeil@cityofpt.us](mailto:mpeil@cityofpt.us)

Service Level Agreement issues:

Caroline Avery, Legal Assistant

(360) 379-5080

[cavery@cityofpt.us](mailto:cavery@cityofpt.us)



WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the City of Port Townsend is hereby amended as follows:

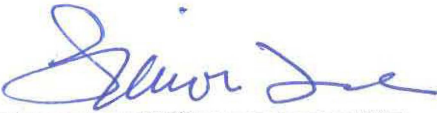
- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.


All other terms and conditions of this Contract remain in full force and effect.

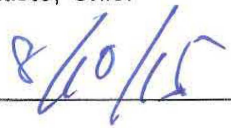
THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

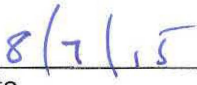
STATE OF WASHINGTON  
WASHINGTON STATE PATROL


CITY OF PORT TOWNSEND

*for*   
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_  
Signature

  
\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Date

Approved as to form  


**SECTOR Service Level Agreement  
Between  
Walla Walla County Prosecuting Attorney's Office  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Walla Walla County Prosecuting Attorney's Office (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.


The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

  
Signature Date 1/27/11

  
Printed Name and Title Jeff Huggins, Contracts MANAGER

WALLA WALLA COUNTY  
PROSECUTING ATTORNEY'S OFFICE

  
Signature Date 1/21/2011

  
Printed Name and Title James L. Nagle Prosecuting Attorney

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.



## APPENDIX C

### Project Contacts

1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

2. For the Agency:

Technical issues and change requests:

Ms. Ann Retzlaff, Legal Assistant

(509) 524-5445

[aretzlaff@co.walla-walla.wa.us](mailto:aretzlaff@co.walla-walla.wa.us)

Service Level Agreement issues:

Mr. James Nagle, County Prosecutor

(509) 524-5445

[Jangle@co.walla-walla.wa.us](mailto:Jangle@co.walla-walla.wa.us)

RECEIVED  
JAN 26 2011  
BUDGET & FISCAL  
WSP

RECEIVED  
MAY 10 2017  
BUDGET & FISCAL  
WSP

WSP Contract No. C110584GSC  
Amendment 1

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Walla Walla County Prosecuting Attorney's Office is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

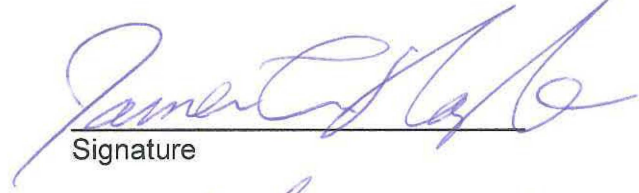
All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

WALLA WALLA COUNTY  
PROSECUTING ATTORNEY'S OFFICE

  
\_\_\_\_\_  
FOR: John R. Batiste, Chief

  
\_\_\_\_\_  
Signature

4/5/17  
\_\_\_\_\_  
Date

March 28, 2017  
\_\_\_\_\_  
Date

**SECTOR Service Level Agreement  
Between  
Whitman County Prosecuting Attorney's Office  
And  
Washington State Patrol**

- 1. Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Whitman County Prosecuting Attorney's Office (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
- 2. Description of SECTOR.** SECTOR has three primary parts:

  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
- 3. Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:

  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
- c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
- d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
- e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
- f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
- g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

*[Handwritten Signature]* *1/27/11*  
\_\_\_\_\_  
Signature Date

*Jeff Hagedahl, Contracts Manager*  
\_\_\_\_\_  
Printed Name and Title

WHITMAN COUNTY PROSECUTING  
ATTORNEY'S OFFICE

*[Handwritten Signature]* *01/20/2011*  
\_\_\_\_\_  
Signature Date

*Ernstine Cooper*  
*Office Administrator*  
\_\_\_\_\_  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.



## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Whitman County Prosecuting Attorney's Office is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

WHITMAN COUNTY PROSECUTING  
ATTORNEY'S OFFICE

  
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_  
Signature

*for*  
\_\_\_\_\_  
Date

*3/31/2017*

\_\_\_\_\_  
Date

*03.31.2017*

**SECTOR Service Level Agreement  
Between  
City of Mercer Island  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Attorney for the City of Mercer Island (acting as prosecutor in the Mercer Island Municipal Court), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;
    - Update required Agency processes with the parameters of SECTOR.

- Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
  - b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.
  - b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.

- c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.
10. **Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.

- 11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.
- 12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.
- 13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.
- 14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF MERCER ISLAND

  
Signature Date 4/14/11

  
Signature Date 4-1-11

Jeff Huggard, Contracts Manager  
Printed Name and Title

Shane Maloney Asst. City Attorney  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

- Appendix A - Statement on Collision Records Data
- Appendix B - SECTOR Governance Committee Training Policies
- Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.



## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the City of Mercer Island is hereby amended as follows:

- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.


*If executed after July 1, 2015, this Amendment is effective retroactive to July 1, 2015, and all intervening acts consistent with this Contract are hereby ratified*  
All other terms and conditions of this Contract remain in full force and effect.

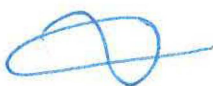
THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

*MD SJ  
-KJ  
7.6.15*

STATE OF WASHINGTON  
WASHINGTON STATE PATROL


CITY OF MERCER ISLAND

*for*   
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_  
Signature

*7-10-15*  
\_\_\_\_\_  
Date

*7/6/15*  
\_\_\_\_\_  
Date

*Approved as to form:*  
 *7.6.15*  
City Attorney

**SECTOR Service Level Agreement**  
**Between**  
**City of Tukwila**  
**And**  
**Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Attorney for the City of Tukwila (acting as prosecutor in the Tukwila Municipal Court under Section 2.16 of the Tukwila Municipal Code), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;
    - Update required Agency processes with the parameters of SECTOR.

- Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.
  - b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.

- c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
- 5. Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
- 6. Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
- 7. Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
- 8. WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
- 9. Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.
- 10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.



## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.



## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the City of Tukwila is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

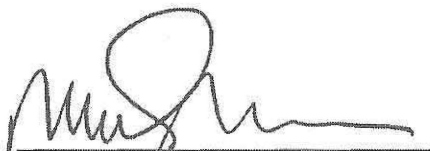


FOR: John R. Batiste, Chief

Date

6-20-17

CITY OF TUKWILA



Signature

Date

6-20-17

**SECTOR Service Level Agreement  
Between  
City of Spokane Prosecutors Office  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the City of Spokane Prosecutors Office (acting as prosecutor in the Spokane Municipal Court under Section 03.01.810 of the Spokane Municipal Code), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;
    - Update required Agency processes with the parameters of SECTOR.

- Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.
  - b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.

- c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.
10. **Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.

- 11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.
- 12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.
- 13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.
- 14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF SPOKANE PROSECUTORS  
OFFICE

Signature

Date

Signature

Date

Printed Name and Title

Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.



## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the City of Spokane Prosecutor's Office is hereby amended as follows:

- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.

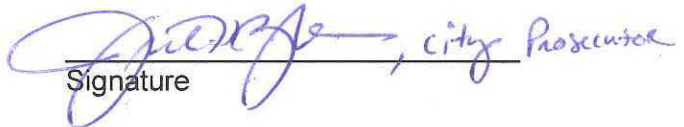
All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF SPOKANE PROSECUTOR'S  
OFFICE

  
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_, City Prosecutor  
Signature

\_\_\_\_\_  
7/30/15  
Date

\_\_\_\_\_  
7/22/15  
Date

**SECTOR Service Level Agreement  
Between  
City of Puyallup  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Attorney for the City of Puyallup (acting as prosecutor in the Puyallup Municipal Court), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;
    - Update required Agency processes with the parameters of SECTOR.

- Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
  - b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.
  - b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.

- c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.
10. **Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.

- 11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.
- 12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.
- 13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.
- 14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF PUYALLUP

Signature

Date

Signature

Date

Printed Name and Title

Printed Name and Title

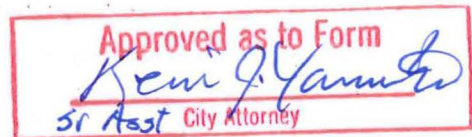
APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts



## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.



## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the City of Puyallup is hereby amended as follows:


- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.


All other terms and conditions of this Contract remain in full force and effect.

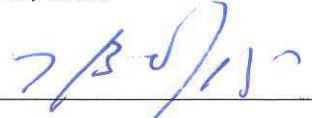
THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF PUYALLUP

  
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_  
Signature  
Steve Kirkubie City Attorney

  
\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Date

**SECTOR Service Level Agreement  
Between  
City of Milton  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Prosecutor for the City of Milton (acting as prosecutor in the Milton Municipal Court), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;
    - Update required Agency processes with the parameters of SECTOR.

- Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
  - b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.
  - b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.

- c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
- 5. Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
- 6. Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
- 7. Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
- 8. WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
- 9. Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.
- 10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.

- 11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.
- 12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.
- 13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.
- 14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF MILTON

*Jeff Hugobald* 3/11/11  
Signature Date

*Krista White-Swain* 2.22.11  
Signature Date

Jeff Hugobald, Contracts Manager  
Printed Name and Title

Krista White-Swain, Prosecutor  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

- Appendix A - Statement on Collision Records Data
- Appendix B - SECTOR Governance Committee Training Policies
- Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.



## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the City of Milton is hereby amended as follows:


- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.

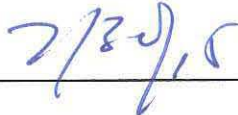
All other terms and conditions of this Contract remain in full force and effect.

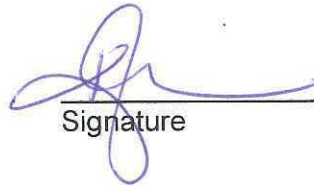
THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF MILTON

  
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Signature

  
\_\_\_\_\_  
Date

**SECTOR Service Level Agreement  
Between  
Langley Police Department  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Langley Police Department (Law Enforcement Agency or LEA). This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
3. **LEA Responsibilities.** The LEA certifies that it operates computers to create vehicle collision reports, NOIs, and NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the LEA are:
  - a. The LEA shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for LEA personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for LEA users and reviewers;
    - Update required LEA processes with the parameters of SECTOR.

- Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. LEA support staff will install SECTOR Client software on LEA-owned equipment. The LEA will not share the SECTOR Client with others.
- c. The LEA acknowledges Appendix A, Statement on Collision Records Data. The LEA certifies that it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements; and that it will not disclose collision data except in compliance with 23 U.S.C. §409, other federal law and state law.
- d. The LEA will adhere to the SECTOR application standards for the computing environment as published by WSP. The LEA will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The LEA will ensure LEA SECTOR equipment maintains current virus checking software. If the LEA SECTOR equipment becomes infected, the LEA will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
- e. LEA users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All LEA users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
- f. The LEA will be responsible for all required hardware and software purchases for the LEA use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including LEA personnel, operating, maintenance, and data transmission costs. Any costs associated with the LEA interfacing with SECTOR BackOffice will be the responsibility of the LEA.

**4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:

- a. WSP will provide SECTOR Client software to the LEA at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the LEA any evasive action required to protect the SECTOR computing environment from significant risk.
- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
- c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.

- d. WSP reserves the right to review and approve LEA equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the LEA in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
- 5. Project Contacts.** WSP and LEA points of contact for this Agreement are identified in Appendix C, Project Contacts.
- 6. Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the LEA. However, the LEA agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The LEA will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
- 7. Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
- 8. WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
- 9. Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or international act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.
- 10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015 or until termination as provided herein.
- 11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for

performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The LEA shall appoint one member to the Dispute Board. The Chief of the WSP and the LEA shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. As an alternative to this process and if applicable, either of the parties may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

Signature

Date

LANGLEY POLICE DEPARTMENT

Signature

Date

Printed Name and Title

Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/22/09

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow LEAs to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

23 U.S.C. §409 prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 [2003]). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.



## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every LEA that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each LEA using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An LEA may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their LEA.
3. Training courses conducted within an LEA must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their LEA should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. LEAs can request assistance from WSP or other agencies for training.
2. LEAs must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the LEA's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each LEA SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the LEA's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## APPENDIX C

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the LEA:

Technical issues and change requests:

Randy Heston, Acting Chief

(360) 221-4433

[pdchief@langleywa.org](mailto:pdchief@langleywa.org)

Service Level Agreement issues:

Randy Heston, Acting Chief

(360) 221-4433

[pdchief@langleywa.org](mailto:pdchief@langleywa.org)

RECEIVED

APR 05 2011

BUDGET & FISCAL  
WSP

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Langley Police Department is hereby amended as follows:

- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.

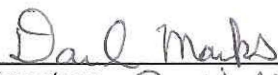
All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

LANGLEY POLICE DEPARTMENT

*for*   
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_  
Signature David Marks, Chief

*7-8-15*  
\_\_\_\_\_  
Date

*6-29-15*  
\_\_\_\_\_  
Date

**SECTOR Service Level Agreement  
Between  
Mountlake Terrace Police Department  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Mountlake Terrace Police Department (Law Enforcement Agency or LEA). This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
3. **LEA Responsibilities.** The LEA certifies that it operates computers to create vehicle collision reports, NOIs, and NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the LEA are:
  - a. The LEA shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for LEA personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for LEA users and reviewers;
    - Update required LEA processes with the parameters of SECTOR.

- Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. LEA support staff will install SECTOR Client software on LEA-owned equipment. The LEA will not share the SECTOR Client with others.
- c. The LEA acknowledges Appendix A, Statement on Collision Records Data. The LEA certifies that it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements; and that it will not disclose collision data except in compliance with 23 U.S.C. §409, other federal law and state law.
- d. The LEA will adhere to the SECTOR application standards for the computing environment as published by WSP. The LEA will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The LEA will ensure LEA SECTOR equipment maintains current virus checking software. If the LEA SECTOR equipment becomes infected, the LEA will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
- e. LEA users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All LEA users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
- f. The LEA will be responsible for all required hardware and software purchases for the LEA use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including LEA personnel, operating, maintenance, and data transmission costs. Any costs associated with the LEA interfacing with SECTOR BackOffice will be the responsibility of the LEA.

**4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:

- a. WSP will provide SECTOR Client software to the LEA at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the LEA any evasive action required to protect the SECTOR computing environment from significant risk.
- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
- c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.

- d. WSP reserves the right to review and approve LEA equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the LEA in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
- 5. Project Contacts.** WSP and LEA points of contact for this Agreement are identified in Appendix C, Project Contacts.
- 6. Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the LEA. However, the LEA agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The LEA will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
- 7. Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
- 8. WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
- 9. Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or international act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.
- 10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015 or until termination as provided herein.
- 11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for

performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

- 12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The LEA shall appoint one member to the Dispute Board. The Chief of the WSP and the LEA shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. As an alternative to this process and if applicable, either of the parties may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.
- 13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.
- 14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

Signature

Date

Printed Name and Title

MOUNTLAKE TERRACE POLICE  
DEPARTMENT

Signature

Date

Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/22/09

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow LEAs to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.



The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

23 U.S.C. §409 prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 [2003]). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every LEA that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each LEA using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An LEA may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their LEA.
3. Training courses conducted within an LEA must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their LEA should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. LEAs can request assistance from WSP or other agencies for training.
2. LEAs must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the LEA's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each LEA SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the LEA's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/feedback to WSP.

## APPENDIX C

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the LEA:

Technical issues and change requests:

Gary Knight, IT Manager

(425) 744-6234

[gknight@ci.mlt.wa.us](mailto:gknight@ci.mlt.wa.us)

Service Level Agreement issues:

Craig McCaul, Commander

(425) 670-8260, ext 4424

[cmccaul@ci28.mlt.wa.us](mailto:cmccaul@ci28.mlt.wa.us)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Mountlake Terrace Police Department is hereby amended as follows:

- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

MOUNTLAKE TERRACE  
POLICE DEPARTMENT



*for* \_\_\_\_\_  
John R. Batiste, Chief

\_\_\_\_\_  
Signature

*7-10-15*  
\_\_\_\_\_  
Date

*07/06/2015*  
\_\_\_\_\_  
Date

**SECTOR Service Level Agreement  
Between  
Bothell Police Department  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Bothell Police Department (Law Enforcement Agency or LEA). This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **LEA Responsibilities.** The LEA certifies that it operates computers to create vehicle collision reports, NOIs, and NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the LEA are:
  - a. The LEA shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for LEA personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for LEA users and reviewers;
    - Update required LEA processes with the parameters of SECTOR.

performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.


- 12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The LEA shall appoint one member to the Dispute Board. The Chief of the WSP and the LEA shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. As an alternative to this process and if applicable, either of the parties may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.
- 13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.
- 14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

BOTHELL POLICE DEPARTMENT

 4/11/11  
Signature Date

 4-4-11  
Signature Date

JEFF HUGHSON, Contracts Manager  
Printed Name and Title

DENISE LANGFORD - CAPTAIN  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/22/09

Appendices:

- Appendix A - Statement on Collision Records Data
- Appendix B - SECTOR Governance Committee Training Policies
- Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow LEAs to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

23 U.S.C. §409 prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 [2003]). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

RECEIVED  
APR 06 2011  
BUDGET & FISCAL  
WSP



## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every LEA that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each LEA using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An LEA may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their LEA.
3. Training courses conducted within an LEA must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their LEA should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. LEAs can request assistance from WSP or other agencies for training.
2. LEAs must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the LEA's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each LEA SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the LEA's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/feedback to WSP.

## APPENDIX C

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the LEA:

Technical issues and change requests:

Brent Meyer, IS Applications Analyst

(425) 489-3377 ext. 5506

[brent.meyer@ci.bothell.wa.us](mailto:brent.meyer@ci.bothell.wa.us)

Service Level Agreement issues:

Denise Langford, Captain

(425) 487-5561

[denise.langford@ci.bothell.wa.us](mailto:denise.langford@ci.bothell.wa.us)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Bothell Police Department is hereby amended as follows:

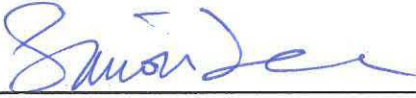
- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.

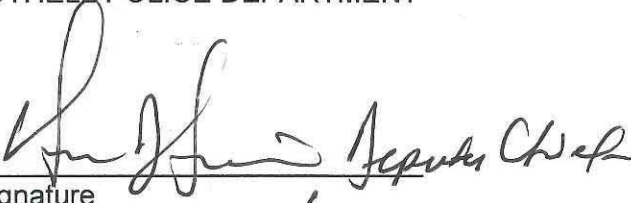
All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

BOTHELL POLICE DEPARTMENT

*for*   
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_  
Signature

7/15/15  
\_\_\_\_\_  
Date

7/7/15  
\_\_\_\_\_  
Date

**SECTOR Service Level Agreement  
Between  
City of East Wenatchee  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Attorney for the City of East Wenatchee (acting as prosecutor in the East Wenatchee Municipal Court), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;
    - Update required Agency processes with the parameters of SECTOR.

- Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.
  - b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.

- c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.
10. **Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.

- 11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.
- 12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.
- 13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement; whether incorporated by reference or otherwise.
- 14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF EAST WENATCHEE

*[Handwritten Signature]* 4/27/11  
Signature Date

*[Handwritten Signature]* 4/13/11  
Signature Date

*Jeff Hochstetler, Contracts Manager*  
Printed Name and Title

*Devin Poulson, City Prosecutor*  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## APPENDIX A

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in



the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

---

2. For the Agency:

Technical issues and change requests:

Joel Rankin

(509) 663-7000

[joelr@keymethod.net](mailto:joelr@keymethod.net)

Service Level Agreement issues:

Devin Poulson, Prosecuting Attorney

(509) 884-9515 ext 116

[dpoulson@east-wenatchee.com](mailto:dpoulson@east-wenatchee.com)

RECEIVED

MAR 19 2011

BUDGET & FISCAL  
WSP

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the City of East Wenatchee is hereby amended as follows:

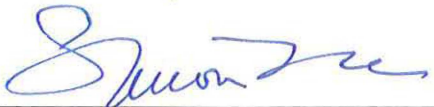
- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.

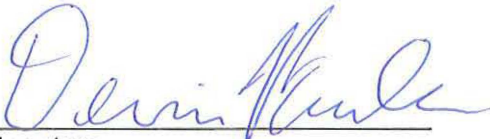
All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF EAST WENATCHEE

*for*   
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_  
Signature

*7/22/15*  
\_\_\_\_\_  
Date

*7/14/15*  
\_\_\_\_\_  
Date

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the City of Pasco is hereby amended as follows:

- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.

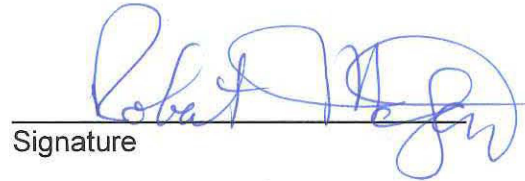
All other terms and conditions of this Contract remain in full force and effect.

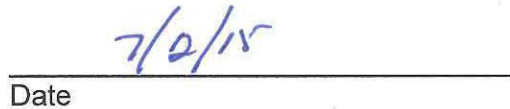
THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

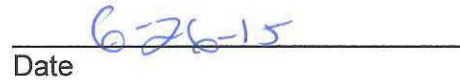
STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF PASCO

  
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_  
Signature

  
\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Date

**SECTOR Service Level Agreement  
Between  
City of Port Angeles  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Attorney for the City of Port Angeles (acting as prosecutor for the City of Port Angeles in Clallam County District Court), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;
    - Update required Agency processes with the parameters of SECTOR.

- Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
- c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
- d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
- e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
- f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
- g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.

**4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:

- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.
- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.

- c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.
10. **Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.



- 11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.
- 12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.
- 13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.
- 14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF PORT ANGELES

|   |  |
|---|--|
|                                    |                              |
| Signature   | Signature  |
| 4/13/11   | 4/13/11  |
| Date  | Date   |
| <br>Jeff Huggins, Contract Manager | <br>Kent Myers, City Manager |
| Printed Name and Title  | Printed Name and Title   |

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

- Appendix A - Statement on Collision Records Data
- Appendix B - SECTOR Governance Committee Training Policies
- Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

Technical issues and change requests:

Bill Creasey, IT

(360) 417-4515

[bcreasey@cityofPA.us](mailto:bcreasey@cityofPA.us)

Service Level Agreement issues:

Dennis Dickson, Assistant City Attorney

(360) 417-4532

[ddickson@cityofPA.us](mailto:ddickson@cityofPA.us)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the City of Port Angeles is hereby amended as follows:

- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.


All other terms and conditions of this Contract remain in full force and effect.

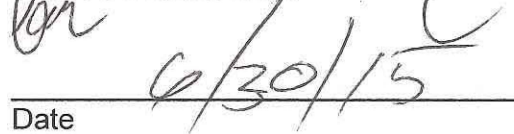
THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

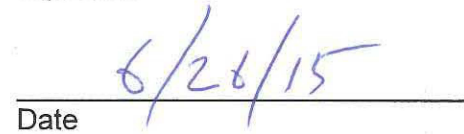
STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF PORT ANGELES

  
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_  
Signature

  
\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Date

# SECTOR Service Level Agreement Between City of Algona And Washington State Patrol

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Attorney for the City of Algona (acting as prosecutor for the City of Algona under the Algona Municipal Code), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;
    - Update required Agency processes with the parameters of SECTOR.

- Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.
  - b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.



- c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
- 5. Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
- 6. Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
- 7. Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
- 8. WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
- 9. Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.
- 10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.

- 11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.
- 12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.
- 13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.
- 14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF ALGONA

Signature

Date

Signature

Date 5/27/11

Printed Name and Title

Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

##### Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

##### Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

##### Technical issues and change requests:

Aaron Walls, Prosecutor

(206) 601-8288

[Aaron@thewallslawfirm.com](mailto:Aaron@thewallslawfirm.com)

##### Service Level Agreement issues:

Aaron Walls, Prosecutor

(206) 601-8288

[Aaron@thewallslawfirm.com](mailto:Aaron@thewallslawfirm.com)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the City of Algona is hereby amended as follows:


- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.

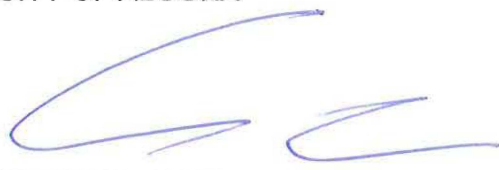
All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF ALGONA

  
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_  
Signature

  
\_\_\_\_\_  
Date

\_\_\_\_\_  
Date

# **SECTOR Service Level Agreement Between City of Orting And Washington State Patrol**

- 1. Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Attorney for the City of Orting (acting as prosecutor for the City of Orting in the Orting Municipal Court), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
- 2. Description of SECTOR.** SECTOR has three primary parts:

  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
- 3. Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:

  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;
    - Update required Agency processes with the parameters of SECTOR.



- Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
  - b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.
  - b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.

- c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
- 5. Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
- 6. Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
- 7. Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
- 8. WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
- 9. Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.
- 10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015, or until termination as provided herein.

- 11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.
- 12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.
- 13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.
- 14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF ORTING

  
Signature Date 6/9/11

  
Signature Date 5/27/11

Jeff Huggins, Contracts Manager  
Printed Name and Title

Aaron Wylie, Prosecutor  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

- Appendix A - Statement on Collision Records Data
- Appendix B - SECTOR Governance Committee Training Policies
- Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## APPENDIX C

### **Project Contacts**

1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

2. For the Agency:

Technical issues and change requests:

Aaron Walls, Prosecutor

(206) 601-8288

[Aaron@thewallslawfirm.com](mailto:Aaron@thewallslawfirm.com)

Service Level Agreement issues:

Aaron Walls, Prosecutor

(206) 601-8288

[Aaron@thewallslawfirm.com](mailto:Aaron@thewallslawfirm.com)

RECEIVED

MAY 31 2011

BUDGET & FISCAL  
WSP

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the City of Orting is hereby amended as follows:

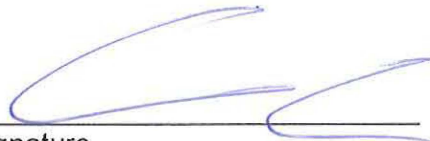
- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF ORTING



for

John R. Batiste, Chief

Signature

Date

10/19/15

Date

10/8/15



**SECTOR Service Level Agreement  
Between  
City of Burien  
And  
Washington State Patrol**

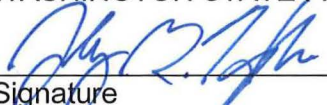
1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Attorney for the City of Burien (acting as prosecutor for the City of Burien under the Burien Municipal Code), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;
    - Update required Agency processes with the parameters of SECTOR.


- 11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.
- 12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.
- 13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.
- 14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF BURIEN

 6/9/11  
Signature Date

  
Signature Date 5/27/11

Jeff Hurdall, Contracts Manager  
Printed Name and Title

Aaron Walls, prosecutor  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

- Appendix A - Statement on Collision Records Data
- Appendix B - SECTOR Governance Committee Training Policies
- Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## APPENDIX C

### Project Contacts

1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

2. For the Agency:

Technical issues and change requests:

Aaron Walls, Prosecutor

(206) 601-8288

[Aaron@thewallslawfirm.com](mailto:Aaron@thewallslawfirm.com)

Service Level Agreement issues:

Aaron Walls, Prosecutor

(206) 601-8288

[Aaron@thewallslawfirm.com](mailto:Aaron@thewallslawfirm.com)

RECEIVED

MAY 31 2011

BUDGET & FISCAL  
WSP

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the City of Burien is hereby amended as follows:

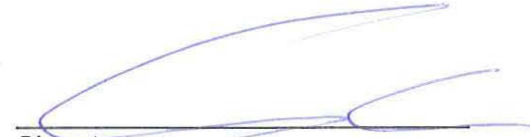
- a. In accordance with Section 11, the period of performance of this Contract is extended until terminated sooner as provided in the Agreement.

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF BURIEN



for

John R. Batiste, Chief

Signature

10/19/15

10/8/15

Date

Date

External Contract Yes  
Comments Non-financial agreement.  
Amendment extends the end date indefinitely

BFS Grants & Contracts Manager Approved Yes  
BFS Budget Analyst Name Shawn Eckhart  
Allotment Needed  
Unanticipated Receipt Needed  
Type of Receipt  
BFS Budget Manager Approved Yes  
Encumber Contract  
BFS Fiscal Analyst Name  
BFS Accounting Manager Approved Yes  
BFS FSP Manager Approved Yes  
BFS Administrator Approved Yes

Questions

Distribute Executed Copies To:

Attachments SECTOR list.xlsx

Version: 4.0

Created at 5/10/2016 4:22 PM by Cline, Karen (WSP)

Last modified at 5/10/2016 5:24 PM by Tee, Simon (WSP)





| Contract Number | Vendor Name                                      | Contact Name                              | Phone Number | E-Mail                              | Address                          | City State Zip             |
|-----------------|--|---|--------------|-------------------------------------|----------------------------------|----------------------------|
| C090871GSC-1    | Washington State Department of Fish and Wildlife | Lieutenant John McIntosh                  | 360-902-2346 | John.McIntosh@dfw.wa.gov            | 600 Capital Way North            | Olympia WA 98501           |
| C090873GSC-1    | Issaquah Police Department                       | Commander Stan Conrad                     | 425-837-3200 | stanc@ci.issaquah.wa.us             | PO Box 1307                      | Issaquah WA 98027          |
| C090874GSC-1    | Skamania County Sheriff's Office                 | Chief Criminal Deputy Pat Bond            | 509-427-9490 | patb@co.skmania.wa.us               | PO Box 790                       | Stevenson WA 98648         |
| C090875GSC-1    | Centralia Police Department                      | Services Commander John Boren             | 360-330-7680 | jboren@cityofcentralia.com          | PO Box 609                       | Centralia WA 98351         |
| C090876GSC-1    | Snoqualmie Police Department                     | Chief of Police James K. Schaffer         | 425-888-3333 | jschaffer@ci.snoqualmie.wa.us       | 34825 SE Douglas Street          | Snoqualmie WA 98065        |
| C090877GSC-1    | Cheney Police Department                         | Commander Rick Campbell                   | 509-498-9285 | rcampbell@cityofcheney.org          | 215 G Street                     | Cheney WA 99004            |
| C090878GSC-1    | Pend Oreille County Sheriff's Office             | Inspector Alan Botzheim                   | 509-447-1901 | Abotzheim@pendoreille.org           | PO Box 5075                      | Newport WA 99156           |
| C090879GSC-1    | Battle Ground Police Department                  | Lieutenant Roy Butler                     | 360-342-5200 | roy.butler@ci.battle-ground.wa.us   | 507 SW 1st Street                | Battle Ground WA 98604     |
| C090881GSC-1    | Airway Heights Police Department                 | Sergeant Robert Swan                      | 509-244-3707 | rswan@cawh.org                      | 1208 S Lundstrom Street          | Airway Heights WA 99001    |
| C090882GSC-1    | Kitsap County Sheriff's Office                   | Lieutenant John Sprague                   | 360-337-4905 | jsprague@co.kitsap.wa.us            | 614 Divison Street               | Port Orchard WA 98366      |
| C090883GSC-1    | Pullman Police Department                        | Commander Chris Tennant                   | 509-334-0802 | chris.tennant@pullman-wa.gov        | 325 SE Paradise Street           | Pullman WA 99163           |
| C090976GSC-1    | Monroe Police Department                         | Administrative Director Debbie Willis     | 360-863-4579 | dwillis@ci.monroe.wa.us             | 818 W Main Street                | Monroe WA 98272            |
| C090977GSC-1    | Chelan County Sheriff's Office                   | Lieutenant Kent Sisson                    | 509-667-6337 | kent.sisson@co.chelan.wa.us         | 401 Washington Street, 1st Level | Wenatchee WA 98801         |
| C090978GSC-1    | Kelso Police Department                          | Mr. Ed Nelson                             | 360-423-1270 | kpdn@kelso.gov                      | PO Box 935                       | Kelso WA 98626             |
| C090979GSC-1    | Walla Walla County Sheriff's Office              | Captain Bill White                        | 509-524-5400 | bwhite@co.walla-walla.wa.us         | 240 W Alder Street               | Walla Walla WA 99362       |
| C090981GSC-1    | Island County Sheriff's Office                   | Sergeant Rick Norrie                      | 360-678-7877 | rickn@co.island.wa.us               | PO Box 5000                      | Coupeville WA 98239        |
| C090982GSC-1    | Mount Vernon Police Department                   | Lieutenant Greg Booth                     | 360-336-6273 | gregb@mountvernonwa.gov             | 1805 Continental Place           | Mount Vernon WA 98273      |
| C090983GSC-1    | Camas Police Department                          | Captain Shyla Nelson                      | 360-817-1524 | snelson@ci.camas.wa.us              | 2100 NE 3rd Avenue               | Camas WA 98607             |
| C090984GSC-1    | Pacific Police Department                        | Detective Steven Churchel                 | 253-929-1130 | schurchel@ci.pacific.wa.us          | 100 3rd Avenue SE                | Pacific WA 98047           |
| C090985GSC-1    | Okanogan County Sheriff's Office                 | Undersheriff Joe Somday                   | 509-422-7200 | jsomday@co.okanogan.wa.us           | 149 N 4th Avenue                 | Okanogan WA 98840          |
| C090986GSC-1    | West Richland Police Department                  | Sergeant Scott Bravo                      | 509-967-3425 | srb@westrichland.org                | 3801 W Van Giesen Street         | West Richland WA 99353     |
| C090987GSC-1    | Whitman County Sheriff's Office                  | Mr. Rick McNannany                        | 509-397-6266 | rickm@co.whitman.wa.us              | PO Box 470                       | Colfax WA 99111            |
| C090988GSC-1    | Blaine Police Department                         | Ms. Lisa Moeller                          | 360-332-6769 | lmoeller@cityofblaine.com           | 322 H Street                     | Blaine WA 98230            |
| C090989GSC-1    | North Bonneville Police Department               | Chief Calvin Owens                        | 509-427-4050 | cal@gorge.net                       | PO Box 7                         | North Bonneville WA 98639  |
| C090990GSC-1    | Lewis County Sheriff's Office                    | Chief Criminal Deputy Gene Seiber         | 360-740-1341 | gene.seiber@lewiscountywa.gov       | 345 West Main Street             | Chehalis WA 98532          |
| C091019GSC-1    | Kirkland Police Department                       | Captain Gene Markle                       | 425-587-3406 | Gmarkle@ci.kirkland.wa.us           | 123 5th Avenue                   | Kirkland WA 98033          |
| C091020GSC-1    | Asotin Police Department                         | Chief Bill Derbonne                       | 509-243-4411 | asotinchief@cablone.net             | PO Box 517                       | Asotin WA 99402            |
| C091021GSC-1    | Bremerton Police Department                      | Chief Craig Rogers                        | 360-473-5220 | craig.rogers@ci.bremerton.wa.us     | 1025 Burwell Street              | Bremerton WA 98337         |
| C100086GSC-1    | Jefferson County Sheriff's Office                | Sergeant Andy Pernsteiner                 | 360-385-3831 | apernsteiner@co.jefferson.wa.us     | 79 Elkins Road                   | Port Hadlock WA 98339      |
| C100087GSC-1    | Lynden Police Department                         | Support Services Manager Marilyn Wyss     | 360-354-2828 | wyssm@lyndenwa.org                  | 203 19th Street                  | Lynden WA 98264            |
| C100144GSC-1    | Bainbridge Island Police Department              | Administrative Lieutenant Sue Schultz     | 206-842-5211 | sschultz@ci.bainbridge-isl.wa.us    | 625 Winslow Way E                | Bainbridge Island WA 98110 |
| C100145GSC-1    | Federal Way Police Department                    | Civilian Operations Manager Cathy Schrock | 253-835-6850 | cathy.schrock@cityoffederalway.com  | PO Box 9718                      | Federal Way WA 98063-9718  |
| C100222GSC-1    | Aberdeen Police Department                       | Sergeant Tom Schmidt                      | 360-538-4444 | tschmidt@apdinfo.com                | 210 E Market Street              | Aberdeen WA 98520          |
| C100311GSC-1    | Poulsbo Police Department                        | Sergeant Howard Lemming                   | 360-779-3113 | hlemming@cityofpoulsbo.com          | PO Box 98                        | Poulsbo WA 98370           |
| C100312GSC-1    | Tieton Police Department                         | Chief Jeff Ketchum                        | 509-673-0200 | tieton601@centurytel.net            | PO Box 357                       | Tieton WA 98947            |
| C100313GSC-1    | Tukwila Police Department                        | Chief David W. Haynes                     | 206-433-1808 |                                     | 6200 Southcenter Boulevard       | Tukwila WA 98188           |
| C100375GSC-1    | Walla Walla Police Department                    | Ms. Patty Blakely                         | 509-524-4377 | pblakely@ci.walla-walla.wa.us       | PO Box 478                       | Walla Walla WA 99362       |
| C100393GSC-1    | Skagit County Sheriff's Office                   | Chief Deputy Tom Molitor                  | 360-336-9450 |                                     | 600 S 3rd Street #100            | Mount Vernon WA 98273      |
| C100470GSC-1    | Arlington Police Department                      | Mr. Seth Kinney                           | 360-403-3400 | skinney@arlingtonwa.gov             | 238 N Olympic Avenue             | Arlington WA 98223         |
| C100471GSC-1    | Coulee Dam Police Department                     | Chief Pat. A. Collins                     | 509-633-1234 | cdpd501@couleedam.org               | 300 Lincoln Avenue               | Coulee Dam WA 99116-1434   |
| C100473GSC-1    | Marysville Police Department                     | Commander Robert Lamoureux                | 360-363-8314 |                                     | 1635 Grove Street                | Marysville WA 98270        |
| C100474GSC-1    | Steilacoom Police Department                     | Sergeant Joshua Billings                  | 253-579-8000 | joshua.billings@ci.steilacoom.wa.us | 601 Main Street                  | Steilacoom WA 98388        |
| C100578GSC-1    | Ruston Police Department                         | Chief Jeremy Kinkel                       | 253-761-0272 | jeremy.kinkel@townofruston.org      | 5117 N Winnifred Street          | Ruston WA 98407            |
| C100641GSC-1    | Covington Police Department                      | Chief Kevin Klason                        | 253-638-1110 | kevin.klason@kingcounty.gov         | 16720 SE 271st Street, Suite 100 | Covington WA 98042         |
| C100642GSC-1    | North Bend Police Department                     | Chief Mark Toner                          | 425-888-4438 | mark.toner@kingcounty.gov           | 1550 Boalch Avenue NW            | North Bend WA 98045        |
| C100726GSC-1    | Snohomish County Sheriff's Office                | Deputy William Ter-Veen                   | 425-388-3829 | william.ter-veen@snoco.org          | 3000 Rockefeller Avenue          | Everett WA 98201           |
| C100781GSC-1    | Brier Police Department                          | Chief Donald E. Lane                      | 425-775-5452 | dlane@cibrier.wa.us                 | 2901 228th Street SW             | Brier WA 98036             |
| C100782GSC-1    | Coupeville Police Department                     | Town Marshal David Penrod                 | 360-678-4461 | paulone@whibey.net                  | PO Box 725                       | Coupeville WA 98239        |
| C100784GSC-1    | Granite Falls Police Department                  | Records Specialist Paula Hutcheson        | 360-691-6611 | pcrouch@granitefallspolice.org      | PO Box 64                        | Granite Falls WA 98252     |
| C100785GSC-1    | Lynnwood Police Department                       | Deputy Chief Karen Manser                 | 425-670-5602 | kmanser@ci.lynnwood.wa.us           | PO Box 5008                      | Lynnwood WA 98046-5008     |
| C100786GSC-1    | Mill Creek Police Department                     | Support Services Manager Robin Swanson    | 425-921-5716 | robin@cityofmillcreek.com           | 15728 Main Street                | Mill Creek WA 98012        |
| C100794GSC-1    | Chewelah Police Department                       | Officer Ryan Pankey                       | 509-935-6555 | Ryanpankey@yahoo.com                | PO Box 258                       | Chewelah WA 99109          |
| C100809GSC-1    | Lakewood Police Department                       | Lieutenant Alex Kasuske                   | 253-830-5000 | akasuske@cityoflakewood.us          | 6000 Main Street SW              | Lakewood WA 98499          |
| C100827GSC-1    | Quincy Police Department                         | Officer Stormy Baughman                   | 509-787-4718 | sbaughman@quincypd.org              | PO Box 426                       | Quincy WA 98848            |
| C100854GSC-1    | Ephrata Police Department                        | Chief Mike Warren                         | 509-754-2491 | mwarren@ephrata.org                 | 121 Alder Street SW              | Ephrata WA 98823           |
| C100993GSC-1    | Westport Police Department                       | Officer Kevin Chaufy                      | 360-268-9197 | kdchaufy@comcast.net                | PO Box 547                       | Westport WA 98595          |
| C110829GSC-1    | Bellingham Police Department                     | Deputy Chief Flo Simon                    | 360-778-8603 | fsimon@cob.org                      | 505 Grand Avenue                 | Bellingham WA 98225        |

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Bellingham Police Department is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.

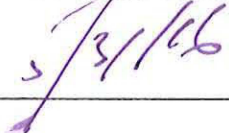
THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

BELLINGHAM POLICE DEPARTMENT



FOR: John R. Batiste, Chief

  
Date

  
Signature *DEPUTY CHIEF*

*5-17-16*  
Date

Washington State Patrol  
**Budget and Fiscal Services Contract Notification Form**

Date 1/17/12  
 TAS   /  /  

|  |  |  |  |  |  |
|--|--|--|--|--|--|
| <input type="checkbox"/> Billable over \$10,000 <input type="checkbox"/> Billable under \$10,000 <input type="checkbox"/> Payable <input checked="" type="checkbox"/> Other: |  |  |  |  |  |
| WSP Contract Number<br>C120470GSC  |  | Other Contract Number                      |  | A/R Number   |  |
| Contract Start Date<br>DOE <u>3/2/12</u>   |  | Contract End Date<br>June 30, 201 <u>5</u> |  | CFDA No.      QFSR<br><input type="checkbox"/> Yes <input type="checkbox"/> No               |  |
| Contract Title<br>SECTOR Service Level Agreement   |  |  |  | Positions hard-coded to contract<br><input type="checkbox"/> Yes <input type="checkbox"/> No |  |
| Contractor Name<br>Department of Natural Resources   |  |  |  |  |  |
| Contractor Contact Address<br>PO Box 47014, Olympia WA 98504-7014  |  |  |  |  |  |
| Contractor Contact Name<br>Officer Jason Bodine  |  | Contractor Contact Phone<br>(360) 628-6930 |  | Contractor EIN/SSN   |  |
| Contractor E-Mail Address<br>jason.bodine@dnr.wa.gov   |  | Contractor Contact Fax                     |  | BFS Accountant Name<br>--  |  |
| WSP Project Manager/Position No.<br>Pat Ramsdell   |  | WSP Section/Division/Bureau<br>ITD         |  | BFS Budget Analyst Name<br>--  |  |

Remarks:

| Contract Amount          |    | Position                     | Signature and Date |
|--------------------------|----|------------------------------|--------------------|
| Previous Contract Amount | \$ | Grants and Contracts Manager |                    |
| Amendment Amount         | \$ | Business Office Manager      |                    |
| Revised Total Amount     | \$ | Budget Manager               |                    |
| Indirect Costs _____%    |    | Accounting Manager           |                    |

Allot:  Yes  No  
 Unanticipated Receipt:  Yes  No

| Master Index | Fund | AI | PI | Project | Sub/<br>subsub<br>Object | Revenue Code |              |            | Billable Code | Percent/<br>Amount |
|--------------|------|----|----|---------|--------------------------|--------------|--------------|------------|---------------|--------------------|
|              |      |    |    |         |                          | Major Group  | Major Source | Sub Source |               |                    |
|              |      |    |    |         |                          |              |              |            |               |                    |
|              |      |    |    |         |                          |              |              |            |               |                    |
|              |      |    |    |         |                          |              |              |            |               |                    |
|              |      |    |    |         |                          |              |              |            |               |                    |

**Billable Contracts Only**

|   |  |
|---|--|
| Mileage Allowed: <input type="checkbox"/> Yes <input type="checkbox"/> No             | Mileage Only: <input type="checkbox"/> Yes <input type="checkbox"/> No               |
| Std Mileage Rate: <input type="checkbox"/> Yes <input type="checkbox"/> No            | Special Mileage Rate \$ _____ per mile   |
| Travel Authorized: <input type="checkbox"/> Yes <input type="checkbox"/> No           | Voluntary O/T: <input type="checkbox"/> Yes <input type="checkbox"/> No              |
| Special Rules: <input type="checkbox"/> Yes <input type="checkbox"/> No               |  |
| Prorate Leave to Contract: <input type="checkbox"/> Yes <input type="checkbox"/> No   | AFRS Code Assigned: <input type="checkbox"/> Yes <input type="checkbox"/> No         |
| Overtime Allowed: <input type="checkbox"/> Yes <input type="checkbox"/> No            | Overtime Only (On Day Off): <input type="checkbox"/> Yes <input type="checkbox"/> No |
| Contract Pays Only O/T Cost: <input type="checkbox"/> Yes <input type="checkbox"/> No | Minimum Call Out Hours: _____  |
| Primary Org Code: _____   | Other Org Codes: _____   |

Type of Receipt:   
 Revenue   
 Interagency Reimbursement   
 Recovery of Expenditure

Distribution:  Project Manager   
 Accountant   
 Budget Analyst   
 Other: \_\_\_\_\_

300-365-522 (R 5/07)



**SECTOR Service Level Agreement  
Between  
Department of Natural Resources  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Department of Natural Resources (a limited authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2016, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.


The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

 3/2/12  
\_\_\_\_\_  
Signature  
Date

  
\_\_\_\_\_  
Printed Name and Title

DEPARTMENT OF NATURAL  
RESOURCES

 2/28/12  
\_\_\_\_\_  
Signature  
Date

  
\_\_\_\_\_  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts



## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## APPENDIX C

### Project Contacts

1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

2. For the Agency:

Technical issues and change requests:

Jarrold Nordloh, Radio Tech

(360) 584-3437

[jarrod.nordloh@dnr.wa.gov](mailto:jarrod.nordloh@dnr.wa.gov)

Service Level Agreement issues:

Officer Jason Bodine

(360) 628-6930

[jason.bodine@dnr.wa.gov](mailto:jason.bodine@dnr.wa.gov)

RECEIVED  
JAN 23 2012  
STATE LANDS DIV

RECEIVED  
MAR 01 2012  
BUDGET & FISCAL  
WSP

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Washington State Department of Natural Resources is hereby amended as follows:

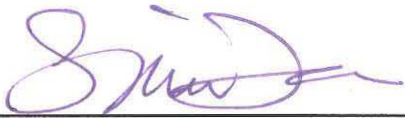
- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

WASHINGTON STATE DEPARTMENT OF  
NATURAL RESOURCES



FOR: John R. Batiste, Chief

  
Signature

Date

5/16/16

Date

MAY 12, 2016

# **SECTOR Service Level Agreement Between Sequim Police Department And Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Sequim Police Department (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington ), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
- c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
- d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
- e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
- f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
- g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.



**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2016, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

SEQUIM POLICE DEPARTMENT

*[Signature]*      1/12/12  
Signature                      Date

*William Dickinson*      01-03-12  
Signature                      Date

*Jeff Hugdahl, Contracts Manager*  
Printed Name and Title

WILLIAM DICKINSON Chief of Police  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

RECEIVED

JAN 09 2012

BUDGET & FISCAL  
WSP

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## APPENDIX C

### Project Contacts

1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

2. For the Agency:

Technical issues and change requests:

Steve Rose, IT Manager

(360) 681-3421

[srose@sequimwa.gov](mailto:srose@sequimwa.gov)

Service Level Agreement issues:

Anthony Graham, Officer

(360) 683-7227

[agraham@ci.sequim.wa.us](mailto:agraham@ci.sequim.wa.us)

RECEIVED

JAN 09 2012

BUDGET & FISCAL  
WSP

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Sequim Police Department is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.


THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

SEQUIM POLICE DEPARTMENT



FOR: John R. Batiste, Chief

  
Signature *CHIEF, SEQUIM POLICE*

6-10-16

Date

06-06-16

Date

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Sequim Police Department is hereby amended as follows:

- a. Appendix C, Section 1 Project Contacts for the Sequim Police Department:

Technical issues and change requests:

Anthony Martin, IT Program Manager  
(360) 582-2444  
[amartin@sequimwa.gov](mailto:amartin@sequimwa.gov)

Service Level Agreement issues:

Devin McBride, Detective  
(360) 582-5723  
[dmcbride@sequimwa.gov](mailto:dmcbride@sequimwa.gov)


All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

SEQUIM POLICE DEPARTMENT

\_\_\_\_\_  
FOR: John R. Batiste, Chief

  
\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

7/21/20  
\_\_\_\_\_  
Date

# SECTOR Service Level Agreement Between Kittitas Police Department And Washington State Patrol

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Kittitas Police Department (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington ), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;



- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2016, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

KITTITAS POLICE DEPARTMENT

Signature

Date

Signature

Date

Printed Name and Title

Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## APPENDIX C

### **Project Contacts**

1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

2. For the Agency:

Technical issues and change requests:

Chris Taylor, Officer

(509) 201-0364

[kpd403@cityofkittitas.com](mailto:kpd403@cityofkittitas.com)

Service Level Agreement issues:

David Anderson, Officer

(509) 929-4340

[kpd402@cityofkittitas.com](mailto:kpd402@cityofkittitas.com)

RECEIVED

JAN 03 2011

BUDGET & FISCAL  
WSP

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Kittitas Police Department is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

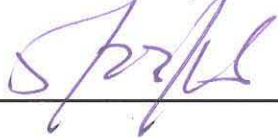
KITTITAS POLICE DEPARTMENT



FOR: John R. Batiste, Chief



Signature



Date



Date



**SECTOR Service Level Agreement  
Between  
City of Federal Way  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Attorney for the City of Federal Way (acting as prosecutor for the City of Federal Way in the Federal Way Municipal Court), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;
    - Update required Agency processes with the parameters of SECTOR.

- Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
  - b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.
  - b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.

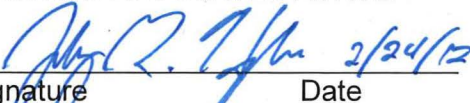
- c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.
10. **Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2016, or until termination as provided herein.


- 11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.
- 12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.
- 13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.
- 14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF FEDERAL WAY

  
Signature Date 2/24/12

  
Signature Date 2/10/12

Jeff Hurdall, Contract Manager  
Printed Name and Title

Patricia Richardson, City Attorney  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

2. For the Agency:

Technical issues and change requests:

Thomas Fichtner, IT Manager

(253) 835-2561

[Thomas.fichtner@cityoffederalway.com](mailto:Thomas.fichtner@cityoffederalway.com)

Service Level Agreement issues:

Tonia Proctor, Lead Paralegal

(253) 835-2561

[Tonia.proctor@cityoffederalway.com](mailto:Tonia.proctor@cityoffederalway.com)

RECEIVED  
FEB 23 2012  
BUDGET & FISCAL  
WSP



WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Federal Way Prosecuting Attorney's Office is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

  
\_\_\_\_\_  
FOR: John R. Batiste, Chief

  
\_\_\_\_\_  
Date

CITY OF FEDERAL WAY

  
\_\_\_\_\_  
Signature / AMY JO PEARSALL, CITY ATTORNEY

  
\_\_\_\_\_  
Date

# **SECTOR Service Level Agreement Between City of SeaTac And Washington State Patrol**

- 1. Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Attorney for the City of SeaTac (acting as prosecutor for the City of SeaTac in the SeaTac Municipal Court), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
- 2. Description of SECTOR.** SECTOR has three primary parts:

  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
- 3. Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:


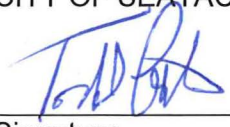


  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;
    - Update required Agency processes with the parameters of SECTOR.

- Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.
  - b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.

- c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
- 5. Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
- 6. Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
- 7. Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
- 8. WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
- 9. Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.
- 10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2016, or until termination as provided herein.

- 11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.
- 12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.
- 13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.
- 14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

|   |   |
|---|---|
| STATE OF WASHINGTON<br>WASHINGTON STATE PATROL  | CITY OF SEATAC  |
|  3/2/12            |  2/23/12      |
| Signature Date  | Signature Date  |
|  Contracts Manager |  City Manager |
| Printed Name and Title  | Printed Name and Title  |

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

Approved as to Form:



## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.



## APPENDIX C

### **Project Contacts**

1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

2. For the Agency:

Technical issues and change requests:

Mike Butay, IT Technician

(206) 973-4888

[mbutay@ci.seatac.wa.us](mailto:mbutay@ci.seatac.wa.us)

Service Level Agreement issues:

Cindy Corsilles, Prosecutor

(206) 973-4630

[ccorsilles@ci.seatac.wa.us](mailto:ccorsilles@ci.seatac.wa.us)

RECEIVED

FEB 29 2012

BUDGET & FISCAL  
WSP

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the SeaTac Prosecuting Attorney's Office is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.


THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.


STATE OF WASHINGTON  
WASHINGTON STATE PATROL

SEATAC PROSECUTING  
ATTORNEY'S OFFICE

  
\_\_\_\_\_  
FOR: John R. Batiste, Chief

  
\_\_\_\_\_  
Signature

  
\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Date

**SECTOR Service Level Agreement  
Between  
Eastern Washington University Police Department  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Eastern Washington University Police Department (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
- 5. Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
- 6. Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
- 7. Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
- 8. WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
- 9. Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2016, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

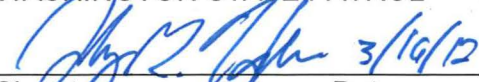
**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

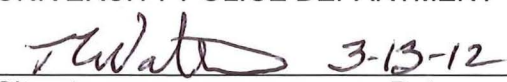
The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

  
Signature Date 3/16/12

Jeff Husdahl, Contracts Manager  
Printed Name and Title

EASTERN WASHINGTON  
UNIVERSITY POLICE DEPARTMENT

  
Signature Date 3-13-12

T. L. WALTERS Chief  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.



## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

2. For the Agency:

Technical issues and change requests:

Dave Stewart, LE IT Tech

(509) 359-2072

[dstewart@ewu.edu](mailto:dstewart@ewu.edu)

Service Level Agreement issues:

Quincy Burns, Detective

(509) 370-5190

[eburns@ewu.edu](mailto:eburns@ewu.edu)

**RECEIVED**  
**MAR 1 6 2012**  
**BUDGET & FISCAL**  
**WSP**

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Eastern Washington University Police Department is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.

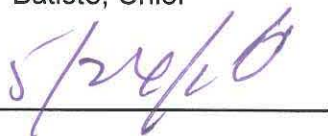
THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL



FOR: John R. Batiste, Chief

Date



EASTERN WASHINGTON UNIVERSITY  
POLICE DEPARTMENT



Signature

5-17-16

Date

**SECTOR Service Level Agreement  
Between  
Klickitat County Sheriff's Office  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Klickitat County Sheriff's Office (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
- 5. Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
- 6. Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
- 7. Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
- 8. WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
- 9. Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2016, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

 4/27/12  
Signature Date

  
Printed Name and Title

KLICKITAT COUNTY SHERIFF'S  
OFFICE

 042312  
Signature Date

Jolene M. Kullio Undersheriff  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in



the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## APPENDIX C

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

Technical issues and change requests:

Pat Kaley, Chief Criminal Deputy

(509) 773-4455

[patk@co.klickitat.wa.us](mailto:patk@co.klickitat.wa.us)

Service Level Agreement issues:

Pat Kaley, Chief Criminal Deputy

(509) 773-4455

[patk@co.klickitat.wa.us](mailto:patk@co.klickitat.wa.us)

**RECEIVED**  
**APR 25 2012**  
**BUDGET & FISCAL**  
**WSP**

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Klickitat County Sheriff's Office is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

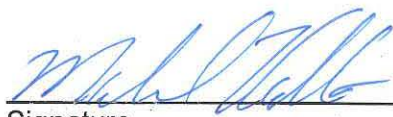
All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

KLICKITAT COUNTY SHERIFF'S OFFICE

\_\_\_\_\_  
FOR: John R. Batiste, Chief

  
\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

5-23-16  
\_\_\_\_\_  
Date

**SECTOR Service Level Agreement  
Between  
Des Moines Police Department  
And  
Washington State Patrol**

- 1. Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Des Moines Police Department (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
- 2. Description of SECTOR.** SECTOR has three primary parts:

  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
- 3. Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:

  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2016, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

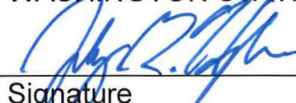
**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

DES MOINES POLICE DEPARTMENT

 3/2/12  
Signature Date

 02/23/12  
Signature Date

Jeff Huskald, Contracts Manager  
Printed Name and Title

John O'Leary  
Chief of Police  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts



## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

**RECEIVED**  
FEB 28 2012  
BUDGET & FISCAL  
WSP

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

Technical issues and change requests:

Dale Southwick, Technology Manager

(206) 870-6545

[dsouthwick@desmoineswa.gov](mailto:dsouthwick@desmoineswa.gov)

Service Level Agreement issues:

Bob Crane, Patrol Officer

(206) 870-7624

[bcrane@desmoineswa.gov](mailto:bcrane@desmoineswa.gov)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Des Moines Police Department is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

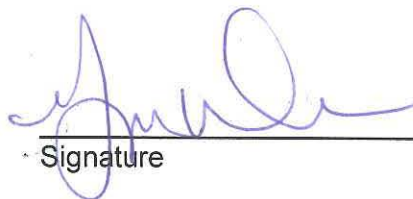


FOR: John R. Batiste, Chief

Date

5/19/16

DES MOINES POLICE DEPARTMENT



Signature

Date

5-16-16

**SECTOR Service Level Agreement  
Between  
Republic Police Department  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Republic Police Department (Law Enforcement Agency or LEA). This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **LEA Responsibilities.** The LEA certifies that it operates computers to create vehicle collision reports, NOIs, and NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the LEA are:
  - a. The LEA shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for LEA personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for LEA users and reviewers;
    - Update required LEA processes with the parameters of SECTOR.

- Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. LEA support staff will install SECTOR Client software on LEA-owned equipment. The LEA will not share the SECTOR Client with others.
  - c. The LEA acknowledges Appendix A, Statement on Collision Records Data. The LEA certifies that it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements; and that it will not disclose collision data except in compliance with 23 U.S.C. §409, other federal law and state law.
  - d. The LEA will adhere to the SECTOR application standards for the computing environment as published by WSP. The LEA will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The LEA will ensure LEA SECTOR equipment maintains current virus checking software. If the LEA SECTOR equipment becomes infected, the LEA will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. LEA users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All LEA users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The LEA will be responsible for all required hardware and software purchases for the LEA use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including LEA personnel, operating, maintenance, and data transmission costs. Any costs associated with the LEA interfacing with SECTOR BackOffice will be the responsibility of the LEA.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the LEA at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the LEA any evasive action required to protect the SECTOR computing environment from significant risk.
  - b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.

- d. WSP reserves the right to review and approve LEA equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the LEA in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and LEA points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the LEA. However, the LEA agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The LEA will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or international act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.
10. **Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2015 or until termination as provided herein.
11. **Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for



performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The LEA shall appoint one member to the Dispute Board. The Chief of the WSP and the LEA shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. As an alternative to this process and if applicable, either of the parties may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

Signature

Date

Printed Name and Title

REPUBLIC POLICE DEPARTMENT

Signature

Date

Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/22/09

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow LEAs to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

23 U.S.C. §409 prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 [2003]). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every LEA that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each LEA using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An LEA may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their LEA.
3. Training courses conducted within an LEA must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their LEA should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. LEAs can request assistance from WSP or other agencies for training.
2. LEAs must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the LEA's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each LEA SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the LEA's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## APPENDIX C

### **Project Contacts**

1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

2. For the LEA:

Technical issues and change requests:

George Bonney, IT Tech

(509) 775-0231

[comptem@rcable.com](mailto:comptem@rcable.com)

Service Level Agreement issues:

Sergeant Ken Marcuson

(509) 775-2812

[officerkenmarcuson@rcabletv.com](mailto:officerkenmarcuson@rcabletv.com)

RECEIVED  
MAY 17 2012  
BUDGET & FISCAL  
WSP

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Republic Police Department is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

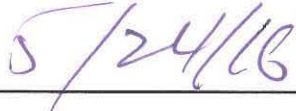
All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL



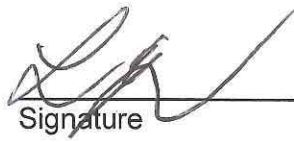
FOR: John R. Batiste, Chief



Date

REPUBLIC POLICE DEPARTMENT

SGT LOREN CULP



Signature



Date

# SECTOR Service Level Agreement Between Kent Police Department And Washington State Patrol

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Kent Police Department (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;
    - Update required Agency processes with the parameters of SECTOR.

- Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.
  - b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.



- c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
- 5. Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
- 6. Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
- 7. Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
- 8. WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
- 9. Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.
- 10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2016, or until termination as provided herein.

- 11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.
- 12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.
- 13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.
- 14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

*Robert Maki*      *6/25/12*  
Signature                      Date

ROBERT MAKI, CFO  
Printed Name and Title

KENT POLICE DEPARTMENT

*Ken Thomas*      *6/25/12*  
Signature                      Date

KEN THOMAS      CHIEF OF POLICE  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## APPENDIX C

### Project Contacts

1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

2. For the Agency:

Technical issues and change requests:

Curt Ryser

(253) 856-4642

[CRyser@kentwa.gov](mailto:CRyser@kentwa.gov)

Service Level Agreement issues:

Sergeant Robert Constant

(253) 856-5882

[rconstant@kentwa.gov](mailto:rconstant@kentwa.gov)

RECEIVED

JUN 26 2012

BUDGET & FISCAL  
WSP

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Kent Police Department is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL



FOR: John R. Batiste, Chief

Date

6/8/16

KENT POLICE DEPARTMENT



Signature

Date

6-4-16

**SECTOR Service Level Agreement  
Between  
Klickitat County Prosecuting Attorney's Office  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Klickitat County Prosecuting Attorney's Office (an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington ), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;
    - Update required Agency processes with the parameters of SECTOR.



- Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.
  - b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.

- c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
- 5. Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
- 6. Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
- 7. Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
- 8. WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
- 9. Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.
- 10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2016, or until termination as provided herein.

- 11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.
- 12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.
- 13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.
- 14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

KLICKITAT COUNTY PROSECUTING  
ATTORNEY'S OFFICE

Signature

Date

Signature

Date

Printed Name and Title

Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## APPENDIX A

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## APPENDIX C

### Project Contacts

1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

2. For the Agency:

Technical issues and change requests:

Summer Beeks, LASA

509-773-5838

[summerz@co.klickitat.wa.us](mailto:summerz@co.klickitat.wa.us)

Service Level Agreement issues:

Lori Lynn Hocht, Prosecutor

509-773-5838

[lorih@co.klickitat.wa.us](mailto:lorih@co.klickitat.wa.us)

RECEIVED

JUN 11 2012

BUDGET & FISCAL  
WSP

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Klickitat County Prosecuting Attorney's Office is hereby amended as follows:

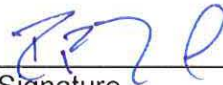
- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: [sectoradmin@wsp.wa.gov](mailto:sectoradmin@wsp.wa.gov)
- c. Appendix C, Section 2 Project Contacts for Service Level Agreement issues:  
David R. Quesnel, Prosecutor  
[davidq@klickitatcounty.org](mailto:davidq@klickitatcounty.org)  
(509) 773-5838  
Technical Issues and Change Requests:  
Tracy L. Hocter, Office Administrator  
(509) 773-5838  
[tracyh@klickitatcounty.org](mailto:tracyh@klickitatcounty.org)  
IT Contact:  
Technical Services Division  
Glen Chipman, Director  
205 S.Columbs Room 103  
Goldendale, WA 98620  
(509) 773-2331  
[glenc@klickitatcounty.org](mailto:glenc@klickitatcounty.org)

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.


STATE OF WASHINGTON  
WASHINGTON STATE PATROL

KLICKITAT COUNTY PROSECUTING  
ATTORNEY'S OFFICE



FOR: John R. Batiste, Chief

Signature



Date

Date



IN WITNESS WHEREOF, the parties here to have signed this agreement this 24<sup>th</sup>  
day of May, 2016

BOARD OF COUNTY COMMISSIONERS  
Klickitat County, Washington

Absent

\_\_\_\_\_  
David M. Sauter, Chairman

Jim Sizemore vice chair  
Jim Sizemore, Commissioner

Rex F. Johnston  
Rex F. Johnston, Commissioner

ATTEST:

Clerk of the Board

[Signature]  
In and for the County of Klickitat,  
State of Washington

APPROVED AS TO FORM:

[Signature]  
David R. Quesnel  
Klickitat County Prosecuting Attorney

**SECTOR Service Level Agreement  
Between  
City of Des Moines  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Attorney for the City of Des Moines (acting as prosecutor in the Municipal Court of the City of Des Moines), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;
    - Update required Agency processes with the parameters of SECTOR.

- Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
  - b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.
  - b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.

- c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
- 5. Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
- 6. Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
- 7. Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
- 8. WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
- 9. Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.
- 10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2016, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF DES MOINES

  
Signature Date 6/29/12

  
Signature Date 6/7/12

Jeff Huschahl, Contracts  
Printed Name and Title MANAGER

Anthony A. Prosecki/City Mgr  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

APPROVED AS TO FORM:  
  
Des Moines City Attorney

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)). Accordingly, collision data may not be disclosed unless a requestor acknowledges that the data will not be used in any action for damages arising from any occurrence at a location mentioned in the report.

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.



## **APPENDIX C**

### **Project Contacts**

1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

2. For the Agency:

Technical issues and change requests:

Chris Pauk

206-870-6721

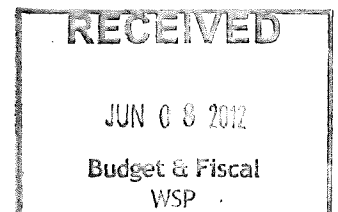
[cpauk@desmoineswa.gov](mailto:cpauk@desmoineswa.gov)

Service Level Agreement issues:

Barry Sellers, Sgt.

206-870-7616

[bsellers@desmoineswa.gov](mailto:bsellers@desmoineswa.gov)



WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Des Moines Prosecuting Attorney's Office is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL



FOR: John R. Batiste, Chief

Date

3/29/17

DES MOINES PROSECUTING  
ATTORNEY'S OFFICE



Signature

Date

3-28-17

# **SECTOR Service Level Agreement Between City of Shelton And Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Attorney for the City of Shelton (acting as prosecutor in the Municipal Court of the City of Shelton), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;
    - Update required Agency processes with the parameters of SECTOR.

- Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
  - b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.
  - b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.

- c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
- 5. Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
- 6. Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
- 7. Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
- 8. WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
- 9. Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.
- 10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2016, or until termination as provided herein.

- 11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.
- 12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.
- 13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.
- 14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF SHELTON

  
Signature Date 8/20/12

  
Signature Date 8/15/12<sup>SE</sup>

 Contracts Manager  
Printed Name and Title

 Sharon English, City Prosecutor  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 6/8/2012

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix B - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in the field, pursuant to federal, state and local requirements. This data is then transferred

to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)).



## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

**APPENDIX C**

**Project Contacts**

1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

2. For the Agency:

Technical issues and change requests:

~~Sharon English, LASA~~

~~360.357.7791~~

~~[senglish@glclaw.com](mailto:senglish@glclaw.com)~~

~~Dan Patton~~

~~602.920.1234~~

Sgt. Harry Heldreth

360 - 432 - 5145

[hheldreth@ci.shelton.wa.us](mailto:hheldreth@ci.shelton.wa.us)

Service Level Agreement issues:

Dan Patton, LASA

360.426.4441

[Daniel@ci.shelton.wa.us](mailto:Daniel@ci.shelton.wa.us)

RECEIVED

AUG 17 2012

BUDGET & FISCAL  
WSP

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

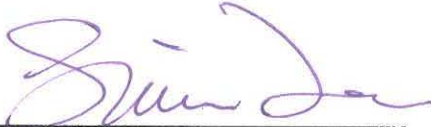
The above-referenced Contract between the Washington State Patrol and the Shelton Prosecuting Attorney's Office is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL



FOR: John R. Batiste, Chief

5/24/16

Date

SHELTON PROSECUTING ATTORNEY'S  
OFFICE

 WSPA# 376052  
Signature Shelton City Prosecutor

5/17/16

Date

**SECTOR Service Level Agreement  
Between  
City of Aberdeen  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the City of Aberdeen (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software.
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
- c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
- d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
- e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
- f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
- g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2017, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

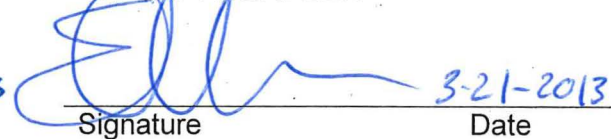
The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

  
Signature Date 4/1/13

ROBERT MAKI, CEO  
Printed Name and Title

CITY OF ABERDEEN

  
Signature Date 3-21-2013

ERIC S. NELSON  
Printed Name and Title

CORPORATION COUNSEL

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix C - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in the field, pursuant to federal, state and local requirements. This data is then transferred



to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)).

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## APPENDIX C

### **Project Contacts**

#### 1. For WSP:

##### Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

##### Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

##### Technical issues and change requests:

Ms. Sandy Mullins

(360) 537-3202

[smullins@aberdeenwa.gov](mailto:smullins@aberdeenwa.gov)

##### Service Level Agreement issues:

Mr. Forest Worgum

(360) 537-3232

[fworgum@aberdeenwa.gov](mailto:fworgum@aberdeenwa.gov)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the City of Aberdeen is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- a. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF ABERDEEN

  
\_\_\_\_\_  
FOR: John R. Batiste, Chief

  
\_\_\_\_\_  
Signature

10-18-17  
\_\_\_\_\_  
Date

10-17-17  
\_\_\_\_\_  
Date

**SECTOR Service Level Agreement  
Between  
Clallam County  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Clallam County Prosecutor (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software.
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2017, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

Signature

Date

Printed Name and Title

*Robert Maki*  
*3/20/13*  
*ROBERT MAKI, CO*

CLALLAM COUNTY

Signature

Date

Printed Name and Title

*[Signature]* *3/18/13*  
*JAMES A. JONES JR* *County Administrator*

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix C - Project Contacts

Approved as to form by:

*[Signature]*  
Mark Nichols  
Chief Deputy Prosecuting Attorney  
Clallam County



## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in the field, pursuant to federal, state and local requirements. This data is then transferred

to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)).

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## APPENDIX C

### **Project Contacts**

#### 1. For WSP:

##### Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

##### Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

##### Technical issues and change requests:

Ms. Deborah Earley, IT Director

(360) 417-2345

[dearly@co.clallam.wa.us](mailto:dearly@co.clallam.wa.us)

##### Service Level Agreement issues:

Ms. Deborah S. Kelly, Deputy Prosecutor

(360) 417-2297

[canderson@co.clallam.wa.us](mailto:canderson@co.clallam.wa.us)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Clallam County Prosecuting Attorney's Office is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL



FOR: John R. Batiste, Chief

6-13-17

Date

CLALLAM COUNTY PROSECUTING  
ATTORNEY'S OFFICE

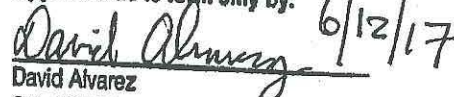


Signature

6.12.17

Date

Approved as to form only by:



David Alvarez  
Chief Civil Deputy Prosecuting Attorney  
Clallam County

**SECTOR Service Level Agreement  
Between  
Lacey Prosecuting Attorney  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Lacey Prosecuting Attorney (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software.
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.



**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2017, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.


**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL  
  
Signature Date 6/17/13  
ROBERT MAKI, CEO  
Printed Name and Title

LACEY PROSECUTING ATTORNEY  
  
Signature Date 6/5/13  
Joseph M. Svoboda, Assistant City Atty  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix C - Project Contacts

## APPENDIX A

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in the field, pursuant to federal, state and local requirements. This data is then transferred

to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)).

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## APPENDIX C

### **Project Contacts**

#### 1. For WSP:

##### Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

##### Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

##### Technical issues and change requests:

Mr. Dave Schneider, City Attorney

(360) 491-1802

[Dave@Laceylawgroup.com](mailto:Dave@Laceylawgroup.com)

##### Service Level Agreement issues:

Mr. Joe Svoboda, City Attorney

(360) 491-1802

[Joe@laceylawgroup.com](mailto:Joe@laceylawgroup.com)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the City of Lacey Prosecuting Attorney's Office is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL



FOR: John R. Batiste, Chief



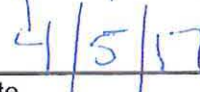
Date

CITY OF LACEY PROSECUTING  
ATTORNEY'S OFFICE



Signature

WSBA 14119



Date

**SECTOR Service Level Agreement  
Between  
City of McCleary  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the City of McCleary (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software.
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.



- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2017, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

Signature

Date

3/18/13

Printed Name and Title

*Robert Maki*  
ROBERT MAKI,  
CFO

CITY OF MCCLEARY

Signature

Date

3-14-2013

Printed Name and Title

*Donald G. Dent*  
Donald Gary Dent  
Mayor

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix C - Project Contacts

## APPENDIX A

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in the field, pursuant to federal, state and local requirements. This data is then transferred

to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)).

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

Technical issues and change requests:

Mr. Randy Bunch

(360) 495-3107

[rbunch@cityofmccleary.com](mailto:rbunch@cityofmccleary.com)

Service Level Agreement issues:

Mr. George Crumb

(360) 495-3107

[georgec@cityofmccleary.com](mailto:georgec@cityofmccleary.com)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT


The above-referenced Contract between the Washington State Patrol and the McCleary Police Department is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.


THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

  
\_\_\_\_\_  
FOR: John R. Batiste, Chief

6-28-2017  
\_\_\_\_\_  
Date

MCCLEARY POLICE DEPARTMENT

  
\_\_\_\_\_  
Signature

6/28/2017  
\_\_\_\_\_  
Date

**SECTOR Service Level Agreement  
Between  
Clark County Prosecuting Attorney  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Clark County Prosecuting Attorney (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software.
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;



- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2017, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

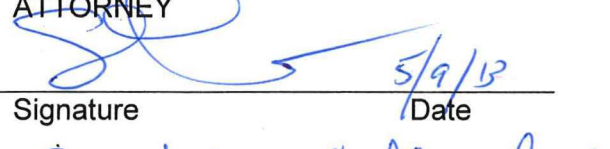
**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL  
  
Signature Date 5/16/13  
ROBERT MAKI, CEO  
Printed Name and Title

CLARK COUNTY PROSECUTING  
ATTORNEY  
  
Signature Date 5/9/13  
Scott Jackson, Chief Criminal DPA  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix C - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in the field, pursuant to federal, state and local requirements. This data is then transferred

to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)).

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

Technical issues and change requests:

Mr. Cliff Anderson,

(360) 397-2261 x 4957

[clifford.anderson@clark.wa.gov](mailto:clifford.anderson@clark.wa.gov)

Service Level Agreement issues:

Ms. Shari Jensen

(360) 397-2261 x 4763

[shari.jensen@clark.wa.gov](mailto:shari.jensen@clark.wa.gov)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Clark County Prosecuting Attorney's Office is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: [sectoradmin@wsp.wa.gov](mailto:sectoradmin@wsp.wa.gov)
- c. Appendix C, Section 2 Project Contracts for Technical issues and change requests:  
Ms. Leslie Ripplinger  
(360) 397-2261 x 4957  
[Leslie.Ripplinger@clark.wa.gov](mailto:Leslie.Ripplinger@clark.wa.gov)

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL



FOR: John R. Batiste, Chief

4/20/17  
Date

CLARK COUNTY PROSECUTING  
ATTORNEY'S OFFICE



Signature

4/17/17  
Date



**SECTOR Service Level Agreement  
Between  
Jefferson County Prosecutor  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Jefferson County Prosecutor (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software.
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2017, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

Robert L. Maki 3/7/13  
Signature Date

ROBERT MAKI, CEO  
Printed Name and Title

JEFFERSON COUNTY PROSECUTOR

Scott W. Ruskens 3/5/13  
Signature Date

Scott W. Ruskens, Prosecuting Attorney  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix C - Project Contacts

Approved as to form only:

David W. Almy  
Jefferson Co. Prosecutor's Office

3/5/2013

Page 4

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in the field, pursuant to federal, state and local requirements. This data is then transferred

to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)).

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

Technical issues and change requests:

Mr. Todd Oberlander

(360) 385-9171

[toberlander@co.jefferson.wa.gov](mailto:toberlander@co.jefferson.wa.gov)

Service Level Agreement issues:

Mr. Scott Rosekrans

(360) 385-9180

[srosekrans@co.jefferson.wa.us](mailto:srosekrans@co.jefferson.wa.us)



WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Jefferson County Prosecuting Attorney's Office is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

JEFFERSON COUNTY PROSECUTING  
ATTORNEY'S OFFICE

  
\_\_\_\_\_  
FOR: John R. Batiste, Chief

  
\_\_\_\_\_  
Signature

  
\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Date

**SECTOR Service Level Agreement  
Between  
Skagit County Prosecutor  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Skagit County Prosecutor (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software.
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2017, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

SKAGIT COUNTY PROSECUTOR

*Robert Maki*      *5/29/13*      *[Signature]*      *5/29/13*  
Signature                      Date                      Signature                      Date

*ROBERT MAKI, CEO*      *Karen Weyman Skagit County*  
Printed Name and Title                      Printed Name and Title  
*Prosecutor*

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

- Appendices:  
Appendix A - Statement on Collision Records Data  
Appendix B - SECTOR Governance Committee Training Policies  
Appendix C - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in the field, pursuant to federal, state and local requirements. This data is then transferred

to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)).

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.



## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

Technical issues and change requests:

Ms. Debi McGrath

(360) 336-9460 x 5847

[debim@co.skagit.wa.us](mailto:debim@co.skagit.wa.us)

Service Level Agreement issues:

Ms. Vickie Maurer

(360) 336-9460 x 7655

[vickiem@co.skagit.wa.us](mailto:vickiem@co.skagit.wa.us)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

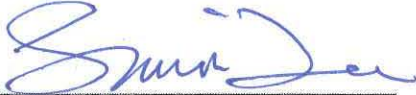
The above-referenced Contract between the Washington State Patrol and the Skagit County Prosecuting Attorney's Office is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL



FOR: John R. Batiste, Chief

6-13-17

Date

SKAGIT COUNTY PROSECUTING  
ATTORNEY'S OFFICE



Signature

6/12/17

Date

**SECTOR Service Level Agreement  
Between  
Auburn Prosecuting Attorney  
And  
Washington State Patrol**

- 1. Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Auburn Prosecuting Attorney (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
- 2. Description of SECTOR.** SECTOR has three primary parts:

  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software.
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
- 3. Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:

  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2017, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.


**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.


The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

  
Signature Date 3/8/13

ROBERT MAKI, CFO  
Printed Name and Title

AUBURN PROSECUTING ATTORNEY

  
Signature Date 3/6/13

Daniel B. Heid City Attorney  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix C - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in the field, pursuant to federal, state and local requirements. This data is then transferred

to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)).



## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

Technical issues and change requests:

Mr. Brian Garbarino

(253) 804-5025

[bgarbarino@auburnwa.gov](mailto:bgarbarino@auburnwa.gov)

Service Level Agreement issues:

Mr. Brian Garbarino

(253) 804-5025

[bgarbarino@auburnwa.gov](mailto:bgarbarino@auburnwa.gov)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

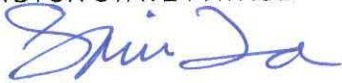
The above-referenced Contract between the Washington State Patrol and the City of Auburn is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov


All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

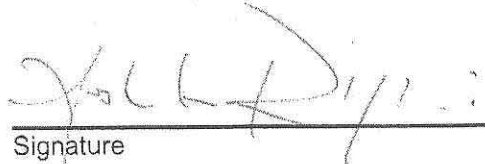


FOR: John R. Batiste, Chief



Date

CITY OF AUBURN



Signature



Date

**SECTOR Service Level Agreement  
Between  
City of Black Diamond  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the City of Black Diamond (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software.
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
4. **WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2017, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

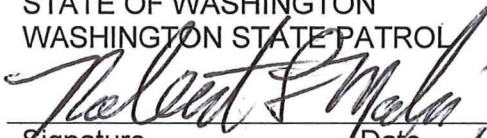
**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

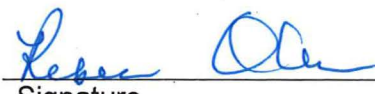
**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

  
Signature \_\_\_\_\_ Date 3/18/13  
ROBERT MALI  
Printed Name and Title \_\_\_\_\_  
CFO

CITY OF BLACK DIAMOND

  
Signature \_\_\_\_\_ Date 3-5-13  
Rebecca Olness, Mayor  
Printed Name and Title \_\_\_\_\_

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix C - Project Contacts

## APPENDIX A

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in the field, pursuant to federal, state and local requirements. This data is then transferred



to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)).

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

Technical issues and change requests:

Mr. Chip Hanson

(253) 631-0351/ (206) 909-2456

[chanson@ci.blackdiamond.wa.us](mailto:chanson@ci.blackdiamond.wa.us)

Service Level Agreement issues:

Chief Jamey Kiblinger

(253) 261-0602

[jkiblinger@police.ci.blackdiamond.wa.us](mailto:jkiblinger@police.ci.blackdiamond.wa.us)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT


The above-referenced Contract between the Washington State Patrol and the Black Diamond Police Department is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

  
\_\_\_\_\_  
FOR: John R. Batiste, Chief

8/10/17  
\_\_\_\_\_  
Date

BLACK DIAMOND POLICE  
DEPARTMENT

  
\_\_\_\_\_  
Signature

8/2/17  
\_\_\_\_\_  
Date

**SECTOR Service Level Agreement  
Between  
Evergreen State College Police Department  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Evergreen State College Police Department (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software.
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
- c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
- d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
- e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
- f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
- g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2017, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

*Robert Magli*      *3/9/13*  
Signature                      Date

*ROBERT MAGLI, CFO.*  
Printed Name and Title

EVERGREEN STATE COLLEGE  
POLICE DEPARTMENT

*Ed Sorger*      *3/11/13*  
Signature                      Date

*Ed Sorger*  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix C - Project Contacts



## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in the field, pursuant to federal, state and local requirements. This data is then transferred

to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)).

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

2. For the Agency:

Technical issues and change requests:

Linda Horn

(360) 887-5512

[hornl@evergreen.edu](mailto:hornl@evergreen.edu)

Service Level Agreement issues:

Linda Horn

(360) 887-5512

[hornl@evergreen.edu](mailto:hornl@evergreen.edu)

WSP Contract No. C130560GSC  
Amendment 1

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Evergreen State College Police Department is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL



FOR: John R. Batiste, Chief

10-16-17

Date

EVERGREEN STATE COLLEGE  
POLICE DEPARTMENT



Signature

10/13/17

Date

**SECTOR Service Level Agreement  
Between  
Colfax Police Department  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Colfax Police Department (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software.
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.



**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2017, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

Robert Maki 3/7/13  
Signature Date

ROBERT MAKI, CFO  
Printed Name and Title

COLFAX POLICE DEPARTMENT

[Signature] 03/07/13  
Signature Date

Rick McManis, Chief of Police  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix C - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in the field, pursuant to federal, state and local requirements. This data is then transferred

to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)).

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

##### Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

##### Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

##### Technical issues and change requests:

Dan Brown

(509) 868-6424

[dbrown@ci.colfax.wa.us](mailto:dbrown@ci.colfax.wa.us)

##### Service Level Agreement issues:

Rick McNannay, Chief of Police

(509) 397-4615

[rmcnannay@ci.colfax.wa.us](mailto:rmcnannay@ci.colfax.wa.us)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Colfax Police Department is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

  
\_\_\_\_\_  
FOR: John R. Batiste, Chief

4-14-2017  
\_\_\_\_\_  
Date

COLFAX POLICE DEPARTMENT

  
\_\_\_\_\_  
Signature

2/4/17  
\_\_\_\_\_  
Date

**SECTOR Service Level Agreement  
Between  
Ocean Shores Police Department  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Ocean Shores Police Department (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
  
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software.
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
  
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.



- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2017, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

Robert Marki 3/7/13  
Signature Date

ROBERT MARKI, CFO  
Printed Name and Title

OCEAN SHORES POLICE  
DEPARTMENT

M. Syner 3/5/13  
Signature Date

MIKE SYNER, CHIEF  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix C - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in the field, pursuant to federal, state and local requirements. This data is then transferred

to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)).

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

Technical issues and change requests:

Sergeant Joe Brouillard

(360) 289-3331 x 121

[brouillard@osgov.com](mailto:brouillard@osgov.com)

Service Level Agreement issues:

Sergeant Don Grossi

(360) 289-3331 x 126

[dgrossi@osgov.com](mailto:dgrossi@osgov.com)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Ocean Shores Police Department is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

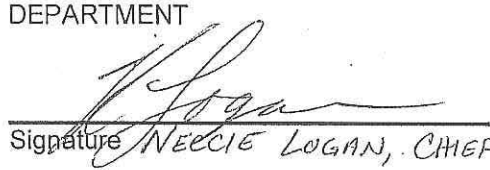
STATE OF WASHINGTON  
WASHINGTON STATE PATROL

  
\_\_\_\_\_  
FOR: John R. Batiste, Chief

Date

4/5/17

OCEAN SHORES POLICE  
DEPARTMENT

  
\_\_\_\_\_  
Signature NEECIE LOGAN, CHIEF of POLICE

Date

4-4-17

# **SECTOR Service Level Agreement Between Selah Police Department And Washington State Patrol**

- 1. Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Selah Police Department (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
- 2. Description of SECTOR.** SECTOR has three primary parts:

  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software.
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
- 3. Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:

  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;



- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2017, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

Signature

Date

Printed Name and Title

SELAH POLICE DEPARTMENT

Signature

Date

Printed Name and Title

*Robert Maki* *5/4/13*  
*Richard D. Hayes* *5/31/13*  
*ROBERT MAKI, CFO* *RICHARD D. HAYES / CHIEF OF POLICE*

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix C - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in

the field, pursuant to federal, state and local requirements. This data is then transferred to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)).

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

2. For the Agency:

Technical issues and change requests:

Stephen Yu

(509) 575-6056

[syu@ci.yakima.wa.us](mailto:syu@ci.yakima.wa.us)

Service Level Agreement issues:

Chief Richard Hayes

(509) 698-7353

[rhayes@ci.selah.wa.us](mailto:rhayes@ci.selah.wa.us)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Selah Police Department is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.


STATE OF WASHINGTON  
WASHINGTON STATE PATROL

  
\_\_\_\_\_  
FOR: John R. Batiste, Chief

Date

  
\_\_\_\_\_

SELAH POLICE DEPARTMENT

  
\_\_\_\_\_  
Signature

Date

  
\_\_\_\_\_



**SECTOR Service Level Agreement  
Between  
Brewster Police Department  
And  
Washington State Patrol**

1. **Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the Brewster Police Department (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
2. **Description of SECTOR.** SECTOR has three primary parts:
  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software.
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
3. **Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:
  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2017, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

BREWSTER POLICE DEPARTMENT

*Robert Maki* 3/11/13

*[Signature]* 030713

Signature

Date

Signature

Date

ROBERT MAKI, CEO

Printed Name and Title

Ken Oakes Chief of Police

Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix C - Project Contacts

## **APPENDIX A**

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in the field, pursuant to federal, state and local requirements. This data is then transferred

to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)).

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.

## **APPENDIX C**

### **Project Contacts**

1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

2. For the Agency:

Technical issues and change requests:

Juana Escobar

(509) 689-2331

[juanaescobar@brewsterpd.org](mailto:juanaescobar@brewsterpd.org)

Service Level Agreement issues:

Rory Williams

(509) 689-2331

[officerwilliams@brewsterpd.org](mailto:officerwilliams@brewsterpd.org)



WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Brewster Police Department is hereby amended as follows:

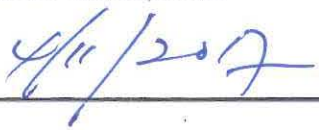
- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.

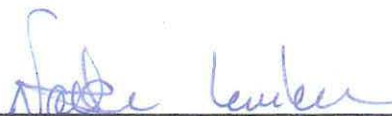
THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.


STATE OF WASHINGTON  
WASHINGTON STATE PATROL

  
\_\_\_\_\_  
FOR: John R. Batiste, Chief

  
\_\_\_\_\_  
Date

BREWSTER POLICE DEPARTMENT

  
\_\_\_\_\_  
Signature Nattalie Cariker, Chief of Police

  
\_\_\_\_\_  
Date

# **SECTOR Service Level Agreement Between City of Napavine And Washington State Patrol**

- 1. Purpose.** This Service Level Agreement (Agreement) is between the Washington State Patrol (WSP) and the City of Napavine (a General authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington; or an Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington), referred to hereafter as the Agency. This Agreement defines roles and expectations in regard to the Statewide Electronic Collision and Ticket Online Records (SECTOR) processes including a method for resolving technical issues.
- 2. Description of SECTOR.** SECTOR has three primary parts:

  - SECTOR Client is the application that operates on a vehicle computer or device, or a collision reviewer's workstation. SECTOR Client software will be used to create and transmit electronic collision reports, notice of infractions (NOI), and notice of criminal citations (NOCC).
  - SECTOR BackOffice is the application and database at WSP that accepts collision reports, NOIs and NOCCs. The SECTOR BackOffice application coordinates updates to the SECTOR Client software.
  - The third part is all applications that receive and process collision, NOI and NOCC data as collected either through SECTOR or on paper forms. These applications are under the control of a governing organization with representatives from the Washington Traffic Safety Commission (WTSC), WSP, the Administrative Office of the Courts (AOC), the Washington State Department of Transportation (WSDOT), and the Department of Licensing (DOL). This group is known as the SECTOR Governance Committee.
- 3. Agency Responsibilities.** The Agency certifies that it operates computers to create or review vehicle collision reports and/or NOIs and/or NOCCs pursuant to federal, state, and local requirements using SECTOR Client. Under this Agreement the responsibilities of the Agency are:

  - a. The Agency shall designate a Local SECTOR Administrator as the primary contact for SECTOR and who will receive SECTOR Administrator training. The Local SECTOR administrator shall:
    - Administer user accounts for Agency personnel;
    - Accept modifications to the SECTOR Client;
    - Document and submit recommendations for modification of SECTOR via the change request process;
    - Manage the connection(s) needed to move data between SECTOR Client to SECTOR BackOffice applications;
    - Provide support for Agency users and reviewers;

- Update required Agency processes with the parameters of SECTOR.
  - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- b. Agency support staff will install SECTOR Client software on Agency-owned equipment. The Agency will not share the SECTOR Client with others.
  - c. The Agency acknowledges Appendix A, Statement on Collision Records Data. The Agency certifies that if it operates electronic equipment to create vehicle collision reports pursuant to federal, state and local requirements it will not disclose collision data except in compliance with federal and state law.
  - d. The Agency will adhere to the SECTOR application standards for the computing environment as published by WSP. The Agency will make its electronic collision, NOI and NOCC reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency SECTOR equipment maintains current virus checking software. If the Agency SECTOR equipment becomes infected, the Agency will take all necessary steps to remove the virus and assure the virus is not transmitted to the SECTOR server located at and maintained by WSP.
  - e. Agency users and reviewers will transfer collisions, NOIs, and NOCCs regularly and promptly. All Agency users and reviewers will adhere to training program detailed in Appendix B, SECTOR Governance Committee Training Policies.
  - f. The Agency will be responsible for all required hardware and software purchases for the Agency use of the SECTOR Client application and the transmittal of collision reports, NOIs, and NOCCs to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with SECTOR BackOffice will be the responsibility of the Agency.
  - g. If the Agency is an Office of a Prosecuting Attorney, Agency users will not utilize the SECTOR client to create collision reports.
- 4. WSP Responsibilities.** WSP provides support for SECTOR Client and SECTOR BackOffice computing environment. Under this Agreement the responsibilities of WSP are:
- a. WSP will provide SECTOR Client software to the Agency at no charge. Maintenance of the SECTOR Client application is provided by WSP, including maintaining compliance with the business rules, data formats, and standardized collision report forms. WSP will provide the Web uniform resource locator (URL) address for connection to the SECTOR BackOffice application and security information to the Local SECTOR Administrator to assure client connectivity. WSP will provide a secure environment for collision, NOI, and NOCC data; and retain this data according to federal and state laws and regulations. WSP will also provide to the Agency any evasive action required to protect the SECTOR computing environment from significant risk.

- b. WSP will create Local SECTOR Administrator Account; train the Local SECTOR Administrator; and assist the Local SECTOR Administrator in administration of agency accounts.
  - c. WSP will provide a change request/control process; coordinate change requests describing issues or enhancements through the SECTOR Governance Committee; provide notification of application modifications; transmit NOIs and NOCCs to AOC; and transmit collision reports to DOT and DOL.
  - d. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
  - e. WSP will support SECTOR Governance Committee sanctioned training.
  - f. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the SECTOR application. This support is limited to resolutions for routine questions on the SECTOR Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP will be moved to a higher level of support within WSP; this higher level of support is provided during regular business hours, Monday through Friday.
5. **Project Contacts.** WSP and Agency points of contact for this Agreement are identified in Appendix C, Project Contacts.
6. **Changes and Modifications.** Except for changes to the points of contact information contained in Appendix C, changes in this Agreement are not in effect unless agreed upon by both WSP and the Agency. However, the Agency agrees to comply with changes in data formats, report forms and other business rules as required by WSP. The Agency will be notified when any changes or updates to these requirements occur. The revising party shall notify the other party of any changes to Appendix C within five (5) business days of the change taking affect.
7. **Compliance with Civil Rights Laws.** During the period of performance for this Agreement, both parties shall comply with all federal and state nondiscrimination laws.
8. **WSP Staffing.** WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.
9. **Hold Harmless.** Each party shall defend, protect and hold harmless the other party from and against all claims suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

**10. Period of Performance.** This Agreement becomes effective on the date of the last signature and continues until June 30, 2017, or until termination as provided herein.

**11. Termination.** Except as otherwise provided in this Agreement, either party may terminate this Agreement by giving ninety (90) calendar days written notification of termination to the other party. If this Agreement is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this Agreement for performance prior to the effective date of termination.

**12. Disputes.** In the event that a dispute arises under this agreement, it shall be determined in the following manner. The Chief of the WSP shall appoint one member to the Dispute Board. The Agency shall appoint one member to the Dispute Board. The Chief of the WSP and the Agency shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto.

**13. Order of Precedence.** In the event of any inconsistency in the terms of this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order: applicable federal and state statutes and regulations; the terms and conditions contained in this Agreement; any other provisions of the Agreement, whether incorporated by reference or otherwise.

**14. Complete Agreement.** This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or bind any of the parties hereto.

The parties signing below warrant that they have read and understand this Agreement; and have the authority to enter into this Agreement.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

CITY OF NAPA VINE

*Robert Maki* 3/11/13  
\_\_\_\_\_  
Signature Date

*John Sayers* 03-05-13  
\_\_\_\_\_  
Signature Date

*ROBERT MAKI, CFO*  
\_\_\_\_\_  
Printed Name and Title

*John Sayers*  
\_\_\_\_\_  
Printed Name and Title

APPROVED BY THE OFFICE OF THE ATTORNEY GENERAL 4/27/2010

Appendices:

Appendix A - Statement on Collision Records Data

Appendix B - SECTOR Governance Committee Training Policies

Appendix C - Project Contacts

## APPENDIX A

### **Statement on Collision Records Data**

In 1938 Washington State law (currently RCW 46.52.060) authorized the Washington State Patrol (WSP) to file, tabulate and analyze collision reports; and to produce certain statistical information about collisions. For the next thirty years WSP maintained a largely manual system for filing collision reports generated over approximately five-year periods. WSP also produced some limited statistical collision data, primarily fatality and accident rate summaries, using paper punch card technology. Analysis of collision data for highway safety purposes was not possible because Washington State did not have a uniform collision report; data on collision reports was primitive and inconsistent; collision reports were not coded by precise roadway location; and no computerized database system existed.

In 1966 and 1973 the federal government enacted laws requiring states to create computerized collision databases in order to analyze the need for highway safety improvements; and to participate in federal programs to fund those improvements. These federal laws and their associated funding provided for states to adopt uniform collision reports containing detailed highway safety coding; and provided that information from these reports would be maintained in a computerized collision database with precise location coding of all collisions. These laws were implemented jointly by WSP and the Washington State Department of Transportation (WSDOT). Beginning in approximately 1970 WSP collected collision reports and entered the raw data into a computer. The data was then transferred to WSDOT for the creation of the collision database required under federal law. WSP maintained copies of individual collision records as well as its database, while WSDOT maintained their own collision database.

The WSP and WSDOT systems for filing individual collision reports, the entry of raw data into a computer, and the creation of the collision database remained unchanged until 1996. By this time the original WSP computer system used for data entry and storage and retrieval of collision records had become obsolete. An attempt to convert to an optical character recognition system was not successful. After an extensive discussion between WSP, WSDOT and the Washington State Office of Financial Management, the agencies concluded that functions related to the maintenance of copies of collision reports and computer input of raw collision report data could be most efficiently performed by WSDOT in conjunction with its already existing collision database function. Beginning in 2002, WSDOT not only created the collision database required by federal law but also, pursuant to an interagency agreement with WSP, began entering all raw collision data into WSDOT's computer. Pursuant to this interagency agreement, WSDOT also began work to develop an electronic imaging system to store and retrieve copies of individual collision reports. This imaging system was implemented in May 2003.

The current system for filing paper collision reports and creating the collision database will remain in effect until WSP, WSDOT and separate law enforcement agencies enter into a SECTOR Service Level Agreement to allow Agencies to file collision reports and transmit collision report data electronically to WSDOT. The Statewide Electronic Collision and Ticket Online Records (SECTOR) application was developed through a collaborative partnership that includes WSP, WSDOT, the Administrative Office of the Courts, the Department of Licensing, and local law enforcement agencies. SECTOR enables law enforcement officers to create electronic collision reports and other forms in the field, pursuant to federal, state and local requirements. This data is then transferred

to a central database where it is available for review, analysis and reporting by law enforcement agencies.

The Department of Licensing is an agency of the State of Washington authorized by law (RCW 46.52.030) to receive full access to collision reports for purposes of maintaining case records under RCW 46.52.120; for supplying abstracts of driving records under RCW 46.52.130; and to administer financial responsibility requirements when drivers are involved in traffic collisions under chapter 46.29 RCW. To perform these functions, they must review collision reports that are filed by law enforcement agencies and citizens.

Federal law prohibits data compiled or collected for purposes of complying with federal highway safety laws from being used in any action for damages arising from any occurrence at a location mentioned in the data (*Pierce County v. Guillen*, 537 U.S. 129 (2003)).

## **APPENDIX B**

### **SECTOR Governance Committee Training Policies**

#### **Training Requirements**

1. Every Agency that elects to use SECTOR must designate one person (up to three) to attend a Governance Team sponsored SECTOR Training Course. This ensures that each Agency using SECTOR will have at least one individual who has received training through the Governance Team sponsored SECTOR Training Course. An Agency may send more than three officers/deputies to Governance Team sponsored SECTOR Training Course when additional seats are available.
2. Individuals who have attended the Governance Team sponsored SECTOR Training Course should assume responsibility for training other users within their Agency.
3. Training courses conducted within an Agency must be coordinated with the SECTOR Training Coordinator.

#### **Training Recommendations**

1. Individuals conducting training within their Agency should be proficient with the SECTOR application prior to training additional users by using SECTOR for at least 90 days prior to conducting training. Agencies can request assistance from WSP or other agencies for training.
2. Agencies must designate a SECTOR point-of-contact through whom all SECTOR support questions will come to the WSP help desk. This point-of-contact will most often be the Agency's designated Local SECTOR Administrator. For urgent SECTOR issues or questions during non-standard work hours SECTOR users may contact the WSP Information Technology Division Customer Services.
3. Each Agency SECTOR User should receive training with the current version of the course materials and according to established course standards. These include:
  - a. Course manuals & exercises
  - b. Training materials
  - c. Suggested course duration (2 days)
  - d. SECTOR Training evaluation form (optional)
4. Individuals who have attended a Governance Team sponsored SECTOR Training Course and are experienced in the use of SECTOR are encouraged to serve as trainers in future Governance Team sponsored SECTOR Training Courses or with other agencies.
5. Recommendations for improvements to SECTOR should be directed to the Agency's Local SECTOR Administrator. The Local SECTOR Administrator sends recommendations/ feedback to WSP.



## **APPENDIX C**

### **Project Contacts**

#### 1. For WSP:

Technical issues and change requests:

Information Technology Division Customer Services Group

Telephone: (360) 705-5999

E-mail: [ITDCustomerServicesGroup@wsp.wa.gov](mailto:ITDCustomerServicesGroup@wsp.wa.gov) or [ITDHelp@wsp.wa.gov](mailto:ITDHelp@wsp.wa.gov)

Service Level Agreement issues:

Ms. Pat Ramsdell

Information Technology Division

Washington State Patrol

Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501

Mailing Address: PO Box 42622, Olympia WA 98504-2622

Telephone: (360) 705-5170

E-mail: [pat.ramsdell@wsp.wa.gov](mailto:pat.ramsdell@wsp.wa.gov)

#### 2. For the Agency:

Technical issues and change requests:

Michael Ellis

(360) 880-0116

[mellis@cityofnapavine.com](mailto:mellis@cityofnapavine.com)

Service Level Agreement issues:

Michael Ellis

(360) 880-0116

[mellis@cityofnapavine.com](mailto:mellis@cityofnapavine.com)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above-referenced Contract between the Washington State Patrol and the Napavine Police Department is hereby amended as follows:

- a. Section 10, the period of performance of this Contract is extended until terminated as provided in accordance with Section 11.
- b. Appendix C, Section 1 Project Contacts for Service Level Agreements issues:  
Ms. Debbie Peterman  
Information Technology Division  
Washington State Patrol  
Street Address: 403 Cleveland Avenue, Suite C, Tumwater WA 98501  
Mailing Address: PO Box 42622, Olympia WA 98504-2622  
Telephone: (360) 596-4976  
E-mail: sectoradmin@wsp.wa.gov

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL



FOR: John R. Batiste, Chief

4/11/2017

Date

NAPAVINE POLICE DEPARTMENT



Signature

4-6-17

Date

RECEIVED

SEP 11 2013

DFI-CONSUMER SERVICES DIVISION  
LICENSING UNIT  
OLYMPIA, WASHINGTON

**MEMORANDUM OF UNDERSTANDING**

**Between the**

**WASHINGTON STATE PATROL**

**And the**

**WASHINGTON STATE  
DEPARTMENT OF FINANCIAL INSTITUTIONS**

**I. PURPOSE**

The parties to this Memorandum of Understanding (MOU) are the Washington State Patrol, Identification and Criminal History Section (WSP) and the Washington State Department of Financial Institutions, a non criminal justice agency (NCJA). This MOU sets forth the policy to ensure the protection of criminal history record information (CHRI) between the WSP, the NCJA, and the Federal Bureau of Investigation (FBI). This MOU provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CHRI data. This policy applies to the NCJA and its contractors with access to, or who operate in support of, non-criminal justice services and information.

**II. ADMINISTRATIVE RESPONSIBILITIES**

As participants in this MOU, the parties will develop mutually and separately appropriate procedures for transmission, dissemination, storage, and destruction of CHRI data.

- a. The Washington State Patrol. WSP shall ensure the NCJA complies with the Criminal Justice Information Services (CJIS) Security Policy (See Exhibit B) which includes authorized use of CHRI, dissemination of CHRI, statute authorization for civil applicant background checks conducted by noncriminal justice agencies, applicant notification and record challenge, security of CHRI, storage of CHRI, outsourcing of noncriminal justice administrative functions, and user fees. WSP will conduct regional audits of all agencies working under this MOU to ensure compliance to all state and federal standards.
- b. NCJA. The NCJA shall be responsible for ensuring:
  1. NCJA responds to requests for information by the FBI CJIS Division or the WSP in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of the agency.
  2. NCJA has formalized written procedures for the following, if applicable: criminal history use and dissemination, misuse, background checks, password management, storage, and destruction of CHRI.
  3. CHRI received as a result of licensing or employment purposes, pursuant to Public Law 92-544 is solely used for the purpose for which the record was requested. Subject fingerprints shall be submitted with all requests for CHRI for noncriminal justice purposes. Access to the FBI CJIS using name-based inquiry and record request messages is not permitted for noncriminal justice purpose, unless otherwise approved by the FBI.
  4. Access to CHRI by authorized officials is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or other authorized entities.

5. All fingerprint based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.
6. NCJA must notify the applicants fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The officials making the determination of suitability for licensing or employment shall provide the applicants the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record. These officials also must advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in Title 28, C.F.R. 16.34. Official making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so.
7. Appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity.
8. NCJA shall seek WSP permission prior to outsourcing noncriminal justice functions.
9. Outsourcing of noncriminal justice administrative functions requiring access to CHRI to either another governmental agency or a private contractor acting as an agent for the authorized receiving agency complies with the security and management control outsourcing standard for non-channelers (see Exhibit A).
10. NCJA is responsible for compliance to technical standards set forth by WSP and the CJIS Security Policy.
11. NCJA will conduct periodic self audits to ensure compliance with CJIS Security Policy.
12. NCJA will participate in WSP and FBI audits, provide plans for any compliance issues, and follow through to resolution within identified timeframes.
13. NCJA will ensure all appropriate staff members are trained according to the state and federal requirements.

### **III. CRIMINAL HISTORY RECORD INFORMATION RESPONSIBILITIES**

NCJA shall conform to system policies, as established by the FBI CJIS Division and WSP, before access to CHRI is permitted. This will allow for control over the data and give assurance of system security.

1. The rules and procedures governing access to CHRI shall apply equally to all participants in the system.
2. All noncriminal justice agencies with access to CHRI data must designate a specific unit, position, or personnel to access CHRI; noncriminal justice agencies must advise WSP of such personnel and changes to such designation.
3. All noncriminal justice agencies with access to CHRI data from the system shall permit an FBI CJIS Division or WSP audit team to conduct appropriate audits. NCJA must cooperate with these audits and respond promptly.

### **IV. SECURITY RESPONSIBILITIES**

#### **Technical Roles and Responsibilities**

NCJA must comply with and enforce system security. NCJA must have someone designated as the security point of contact (POC). Security POC's shall be responsible for the following:

1. Identifying the user of the hardware/software and ensuring that no unauthorized users have access to the same.
2. Identifying and documenting how the equipment is connected to the state system.

**RECEIVED**

**SEP 11 2013**

3. Ensuring that personnel security screening procedures are being followed as stated in the CJIS Security Policy.
4. Ensuring that appropriate hardware security measures are in place.
5. Supporting policy compliance and keeping the WSP informed of security incidents.
6. If the technical POC changes at your agency, notify WSP immediately.

**Security Enforcement**

NCJA is responsible for enforcing system security standards for their agency, in addition to all of the other agencies to which the NCJA provides CHRI information. Authorized users shall access and disseminate the CHRI data only for the purpose for which they are authorized. NCJA shall have a written policy for the discipline of policy violators.

**Technical Security Training**

All Information Technology (IT) employees who have access to and those who have direct responsibility to configure and maintain FBI CJIS systems must review security awareness training within six months of their appointment or assignment. Documentation pertaining to the materials used and those employees which receive security awareness training shall be maintained in a current status.

**Physical Security**

A physically secured location in a noncriminal justice facility, an area, a room, a group of rooms, that is/are subject to criminal justice agency management control security addendum and which contain hardware, software, and/or firmware (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch panels, etc.) that provide access to the CJIS sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that restrict unauthorized access.

All personnel with access to computer centers, CHRI, or areas where CHRI information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check. All personnel must review security awareness training within six months of their appointment or assignment.

**Personnel Security**

To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days of initial employment or assignment for all personnel who have authorized access to FBI CJIS information and those who have direct responsibility to configure and maintain computer systems and networks with access to FBI CJIS information. All requests from system access shall be made as specified by the CJIS Systems Officer (i.e. WSP Identification and Criminal History Section).

- c. NCJA shall use the data supplied by WSP and the FBI under this MOU only for the authorized purpose intended. NCJA shall not use this data for any other purpose and shall not disseminate this data with any other parties unless required by law. NCJA shall share any public disclosure requests regarding this data with the WSP.

**Storage**

Please see 'Security and Management Control Outsourcing Standard for Non-Channelers' (Exhibit A).

RECEIVED

SEP 11 2013

DFI-CONSUMER SERVICES DIVISION  
LICENSING UNIT  
OLYMPIA, WASHINGTON

**V. LIAISON REPRESENTATIVES**  
**For the Washington State Patrol:**

Jim Anderson, Administrator  
Criminal Records Division  
PO Box 42619  
Olympia WA 98504-2619  
Phone: (360) 534-2101  
Fax: (360) 534-2070  
E-mail: [jim.anderson@wsp.wa.gov](mailto:jim.anderson@wsp.wa.gov)

**For the Washington State**  
**Department of Financial Institutions:**

Maureen Camp  
PO Box 41200  
Olympia WA 98504-1200  
360-664-7887  
[maureen.camp@dfi.wa.gov](mailto:maureen.camp@dfi.wa.gov)

**VI. INDEMNIFICATION**

Each party shall defend, protect and hold harmless the other party from and against all claims, suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing this MOU.

**VII. PERIOD OF MOU**

This MOU becomes effective on the date of the last signature and continues for three years and may be renewed. It may be modified by mutual written consent of the two agencies. Liaison Representatives may modify Exhibit A by mutual written consent of the two agencies without changing the general conditions of this MOU.

**VIII. TERMINATION**

Except as otherwise provided in this MOU, either party may terminate this MOU upon ninety (90) days' written notification to the other party. If this MOU is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this MOU for performance prior to the effective date of termination.

**IX. DISPUTES**

In the event that a dispute arises under this MOU, it shall be determined in the following manner: The Chief of WSP, or designee, shall appoint one member to the Dispute Board. NCJA shall appoint one member to the Dispute Board. The Chief of WSP, or designee, and the NCJA shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. If applicable and as an alternative to this process, either of the parties may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.

**X. EXHIBITS**

The exhibits listed below are incorporated into and made a part of this MOU:

Exhibit A - 'Security and Management Control Outsourcing Standard for Non-Channelers'

Exhibit B - Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.2, published 8/9/2013 which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

**RECEIVED**

**SEP 11 2013**

DFI-CONSUMER SERVICES DIVISION  
LICENSING UNIT  
OLYMPIA, WASHINGTON

**XI. ORDER OF PRECEDENCE**

In the event of any inconsistency in the terms of this MOU, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

- a. Applicable federal and state statutes and regulations;
- b. The Terms and Conditions contained in this MOU;
- c. The Exhibits attached to this MOU;
- d. Any other provisions of the MOU, whether incorporated by reference or otherwise.

**XII. ALL WRITINGS CONTAINED HEREIN**

This MOU contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this MOU shall be deemed to exist or to bind any of the parties hereto.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

  
\_\_\_\_\_  
John R. Batiste, Chief

\_\_\_\_\_  
9/20/13  
Date

WASHINGTON STATE  
DEPARTMENT OF FINANCIAL  
INSTITUTIONS

  
\_\_\_\_\_  
Lorenda Lillard

\_\_\_\_\_  
Sept. 19, 2013  
Date

**RECEIVED**

**SEP 11 2013**

DFI-CONSUMER SERVICES DIVISION  
LICENSING UNIT  
OLYMPIA, WASHINGTON

**SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD for  
NON-CHANNELERS**

The goal of this document is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the Contractor. Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security and Management Control Outsourcing Standard (Outsourcing Standard) is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI without a direct connection to the FBI CJIS Wide Area Network (WAN).

**1.0 Definitions**

- 1.01 *Access to CHRI* means to view or make use of CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by title 42, United States Code, section 14614(b).
- 1.02 *Authorized Recipient* means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.
- 1.03 *Chief Administrator* means the primary administrator of a Nonparty State’s criminal history record repository or a designee of such administrator who is



a regular full-time employee of the repository, which is also referred to as the State Identification Bureau (SIB) Chief.

- 1.04 *CHRI*, as referred to in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.
- 1.05 *Criminal History Record Check*, for purposes of this Outsourcing Standard only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.
- 1.06 *Compact Officer*, as provided in Article I(2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the compact among federal agencies], or (B) with respect to a Party State, the chief administrator of the State's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.
- 1.07 *Contractor* means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI.
- 1.08 *Dissemination* means the disclosure of CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 1.09 *Noncriminal Justice Administrative Functions* means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:
1. Making fitness determinations/recommendations
  2. Obtaining missing dispositions
  3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General
  4. Other authorized activities relating to the general handling, use, and storage of CHRI

- 1.10 *Noncriminal Justice Purposes*, as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.
- 1.11 *Outsourcing Standard* means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. This Outsourcing Standard authorizes access to CHRI for noncriminal justice purposes, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.
- 1.12 *Physically Secure Location* means a facility or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CHRI and associated information systems.
- 1.13 *Positive Identification*, as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints<sup>1</sup> or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other non-unique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.
- 1.14 *Public Carrier Network* means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: Dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.
- 1.15 *Security Violation* means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in

---

<sup>1</sup> The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning positive identification may be obtained from the FBI Compact Council office.

violation of: (A) Federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

2.0 *Responsibilities of the Authorized Recipient*

- 2.01 Prior to engaging in outsourcing any noncriminal justice administrative functions, the Authorized Recipient shall: (a) Request and receive written permission from (1) the State Compact Officer/Chief Administrator<sup>2</sup> or (2) the FBI Compact Officer<sup>3</sup>; (b) provide the Compact Officer/Chief Administrator copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested; and (c) inquire of the FBI Compact Officer whether a prospective Contractor has any security violations (See Section 8.04). The FBI Compact Officer will report those findings to the Authorized Recipient and, when applicable, to the State Compact Officer/Chief Administrator.
- 2.02 The Authorized Recipient shall execute a contract or agreement prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.
- 2.03 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; limit retention of the information to a period of time not to exceed that period of time the Authorized Recipient is permitted to retain such information; prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General; ensure the security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; and ensure that Contractor

---

<sup>2</sup>The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and Authorized Recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.

<sup>3</sup>State or local Authorized Recipients based on State or Federal Statutes shall contact the State Compact Officer/Chief Administrator. Federal or Regulatory Agency Authorized Recipients shall contact the FBI Compact Officer.

personnel comply with this Outsourcing Standard.

- a. The Authorized Recipient shall conduct criminal history record checks of Contractor personnel having access to CHRI if such checks are required or authorized of the Authorized Recipient's personnel having similar access.<sup>4</sup> The Authorized Recipient shall maintain updated records of Contractor personnel who have access to CHRI and update those records within 24 hours when changes to that access occur and, if a criminal history record check is required, the Authorized Recipient shall maintain a list of Contractor personnel who successfully completed the criminal history record check.
  - b. The Authorized Recipient shall ensure that the Contractor maintains site security.
  - c. The Authorized Recipient shall ensure that the most current version of both the Outsourcing Standard and the CJIS Security Policy are incorporated by reference at the time of contract, contract renewal, or within 30 calendar days (unless otherwise directed) of notification of successor versions of the Outsourcing Standard and/or CJIS Security Policy, whichever is sooner. The Authorized Recipient shall notify the Contractor within 30 calendar days (unless otherwise directed) of FBI notification regarding changes or updates to the Outsourcing Standard and/or CJIS Security Policy.
- 2.04 The Authorized Recipient shall understand the communications and record capabilities of the Contractor which has access to federal or state records through, or because of, its outsourcing relationship with the Authorized Recipient. The Authorized Recipient shall maintain an updated topological drawing which depicts the interconnectivity of the Contractor's network configuration.
- 2.05 The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the Outsourcing Standard. The Authorized Recipient shall certify to the Compact Officer/Chief Administrator that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.

---

<sup>4</sup>If a national criminal history record check of Authorized Recipient personnel having access to CHRI is mandated or authorized by a federal statute, executive order, or state statute approved by the Attorney General under Public Law 92-544, the State Compact Officer/Chief Administrator and/or the FBI Compact Officer must ensure Contractor personnel having similar access are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives. The national criminal history record checks of Contractor personnel with access to CHRI cannot be outsourced and must be performed by the Authorized Recipient.

2.06 The Authorized Recipient shall provide written notice of any early voluntary termination of the contract to the Compact Officer/Chief Administrator or the FBI Compact Officer.

3.0 *Responsibilities of the Contractor*

3.01 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the CJIS Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

3.02 The Contractor shall develop, document, administer, and maintain a Security Program (Physical, Personnel, and Information Technology) to comply with the most current Outsourcing Standard and the most current FBI *CJIS Security Policy*. The Security Program shall describe the implementation of the security requirements described in this Outsourcing Standard and the FBI *CJIS Security Policy*. In addition, the Contractor is also responsible to set, maintain, and enforce the standards for the selection, supervision, and separation of personnel who have access to CHRI. The Authorized Recipient shall provide the written approval of a Contractor's Security Program.

3.03 The requirements for a Security Program should include, at a minimum:

- a) Description of the implementation of the security requirements described in this Outsourcing Standard and the *CJIS Security Policy*.
- b) Security Training.
- c) Guidelines for documentation of security violations.
- d) Standards for the selection, supervision, and separation of personnel with access to CHRI.

\*\*If the Contractor is using a corporate policy, it must meet the requirements outlined in this Outsourcing Standard and the *CJIS Security Policy*. If the corporate policy is not this specific, it must flow down to a level where the documentation supports these requirements.

3.04 Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. The Authorized Recipient shall review and provide to the Contractor written approval of the Security Training Program. Training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall annually, not later than the anniversary date of the contract, certify in writing to the Authorized Recipient that annual refresher training was completed for those Contractor personnel with access

to CHRI.

- 3.05 The Contractor shall make its facilities available for announced and unannounced audits performed by the Authorized Recipient, the state, or the FBI on behalf of the Compact Council.
- 3.06 The Contractor's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI CJIS Division. During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.
- 3.07 The Contractor shall maintain CHRI only for the period of time necessary to fulfill its contractual obligations but not to exceed the period of time that the Authorized Recipient is authorized to maintain and does maintain the CHRI.
- 3.08 The Contractor shall maintain a log of any dissemination of CHRI, for a minimum of 365 days.

#### 4.0 *Site Security*

- 4.01 The Authorized Recipient shall ensure that the Contractor site(s) is a physically secure location to protect against any unauthorized access to CHRI.

#### 5.0 *Dissemination*

- 5.01 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 5.02 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) The Authorized Recipient and the secondary recipient with unique identifiers, (B) the record disseminated, (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.
- 5.03 If CHRI is stored or disseminated in an electronic format, the Contractor shall protect against unauthorized access to the equipment and any of the data. In no event shall responses containing CHRI be disseminated other than as governed by this Outsourcing Standard or more stringent contract requirements.

#### 6.0 *Personnel Security*

- 6.01 If a local, state, or federal written standard requires or authorizes a criminal history record check of the Authorized Recipient's personnel with access to

CHRI, then a criminal history record check shall be required of the Contractor's (and approved Sub-Contractor's) employees having access to CHRI. Criminal history record checks of Contractor and approved Sub-Contractor employees, at a minimum, will be no less stringent than criminal history record checks that are performed on the Authorized Recipient's personnel performing similar functions. Criminal history record checks must be completed prior to accessing CHRI under the contract.

- 6.02 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm in writing that each employee has certified in writing that he/she understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities. The Contractor shall maintain the employee certifications in a file that is subject to review during audits. Employees shall make such certification prior to performing work under the contract.
- 6.03 The Contractor shall maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur, and if a criminal history record check is required, maintain a list of personnel who have successfully completed criminal history record checks. The Contractor shall notify Authorized Recipients within 24 hours when additions or deletions occur.

7.0 *System Security*

- 7.01 The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy.
- a. If CHRI can be accessed by unauthorized personnel via Wide Area Network/Local Area Network or the Internet, then the Contractor shall protect the CHRI with firewall-type devices to prevent such unauthorized access. These devices shall implement a minimum firewall profile as specified by the CJIS Security Policy in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.
  - b. Data encryption shall be required throughout the network passing CHRI through a shared public carrier network.
- 7.02 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.
- a. CHRI shall be stored in a physically secure location.
  - b. The Authorized Recipient shall ensure that a procedure is in place for

sanitizing all fixed storage media (e.g., disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal, or reuse. Sanitization procedures include overwriting the media and/or degaussing the media.

- c. The Authorized Recipient shall ensure that a procedure is in place for the disposal or return of all non-fixed storage media (e.g., hard copies, print-outs).

7.03 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient, Contractor, or sub-Contractor must be assigned a unique identifying number.

## 8.0 *Security Violations*

### 8.01 Duties of the Authorized Recipient and Contractor

- a. The Contractor shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference.
- b. Pending investigation, the Contractor shall, upon detection or awareness, suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.
- c. The Contractor shall immediately (within four hours) notify the Authorized Recipient of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. Within five calendar days of such notification, the Contractor shall provide the Authorized Recipient a written report documenting such security violation, any corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.
- d. The Authorized Recipient shall immediately (within four hours) notify the State Compact Officer/Chief Administrator and the FBI Compact Officer of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator, if applicable, and the FBI Compact Officer, within five calendar days of receipt of the written report from the Contractor. The written report must include any corrective actions taken by the Contractor and the Authorized Recipient to resolve such security violation.



- 8.02 Termination of the contract by the Authorized Recipient for security violations
- a. The contract is subject to termination by the Authorized Recipient for security violations involving CHRI obtained pursuant to the contract.
  - b. The contract is subject to termination by the Authorized Recipient for the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.
  - c. If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient shall terminate the contract.
- 8.03 Suspension or termination of the exchange of CHRI for security violations
- a. Notwithstanding the actions taken by the State Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Compact Council or the United States Attorney General may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 CFR §906.2(d).
  - b. If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United States Attorney General by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be deleted or returned in accordance with the provisions and time frame as specified by the Authorized Recipient.
- 8.04 The Authorized Recipient shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following:
- a. The termination of a contract for security violations.
  - b. Security violations involving the unauthorized access to CHRI.
  - c. The Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.
- 8.05 The Compact Officer/Chief Administrator, Compact Council and the United States Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.
- 8.06 The Compact Officer/Chief Administrator, Compact Council, and the United

States Attorney General reserve the right to audit the Authorized Recipient and the Contractor's operations and procedures at scheduled or unscheduled times. The Compact Council, the United States Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the contract.

9.0 *Miscellaneous Provisions*

- 9.01 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, Compact Officer/Chief Administrator (where applicable), and the FBI.
- 9.02 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) The CJIS Security Policy.
- 9.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and the CHRI accessed therefrom and it is understood that there may be terms and conditions of the appended contract which impose more stringent requirements upon the Contractor.<sup>5</sup>
- 9.04 The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. Conformance to such security measures may not be less stringent than stated in this Outsourcing Standard without the consent of the Compact Council in consultation with the United States Attorney General.
- 9.05 This Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.
- 9.06 Appropriate notices, assurances, and correspondence to the FBI Compact Officer, Compact Council, and the United States Attorney General required by Section 8.0 of this Outsourcing Standard shall be forwarded by First Class Mail to:
- FBI Compact Officer  
1000 Custer Hollow Road  
Module D-3  
Clarksburg, WV 26306

10.0 *Exemption from Above Provisions*

---

<sup>5</sup>Such conditions could include additional audits, fees, or security requirements. The Compact Council, Authorized Recipients, and the Compact Officer/Chief Administrator have the explicit authority to require more stringent standards than those contained in the Outsourcing Standard.

- 10.01 An Information Technology (IT) contract need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:
1. Access to CHRI by the IT contractor's personnel is limited solely for the development and/or maintenance of the Authorized Recipient's computer system;
  2. Access to CHRI is incidental, but necessary, to the duties being performed by the IT contractor;
  3. The computer system resides within the Authorized Recipient's facility;
  4. The Authorized Recipient's personnel supervise or work directly with the IT contractor personnel;
  5. The Authorized Recipient maintains complete, positive control of the IT contractor's access to the computer system and CHRI contained therein; and
  6. The Authorized Recipient retains all of the duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard.

10.02 An Authorized Recipient's contract where access to CHRI is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 4.0, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:

1. Access to CHRI by the Contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient;
2. Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor;

RECEIVED

SEP 11 2013

3. The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the Authorized Recipient;
4. The Contractor's personnel are subject to the same criminal history record checks as the Authorized Recipient's personnel;
5. The criminal history record checks of the Contractor personnel are completed prior to work on the contract or agreement;
6. The Authorized Recipient retains all other duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard; and
7. The Contractor stores the CHRI in a physically secure location.

**RECEIVED**

**SEP 11 2013**

DFI-CONSUMER SERVICES DIVISION  
LICENSING UNIT  
OLYMPIA, WASHINGTON

RECEIVED  
SEP 11 2013  
BUDGET & FISCAL  
WSR

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above referenced Contract between the Washington State Patrol and Washington State Department of Financial Institutions is hereby amended as follows:

- The end date shall be extended through September 19, 2021.
- EXHIBIT B CJIS Security Policy 5.1 shall be replaced with EXHIBIT B CJIS Security Policy 5.5.

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL



FOR: John R. Batiste, Chief

1/18/17  
Date

WASHINGTON STATE DEPARTMENT  
OF FINANCIAL INSTITUTIONS



Signature  
Director of Consumer Services

January 4, 2017  
Date

WSP Contract No. C130697GSC  
Amendment 1  
WA State Department of Health – N20392  
Amendment 1

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above referenced Contract between the Washington State Patrol and Washington State Department of Health is hereby amended as follows:

- The end date shall be extended through June 30, 2020.
- **Exhibit B** "CJIS Security Policy" shall be replaced by **Exhibit B** – Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.5, published 6/1/2016 which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

All other terms and conditions of this Contract remain in full force and effect.

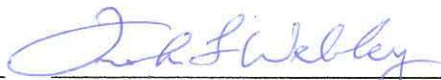
THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

STATE OF WASHINGTON  
DEPARTMENT OF HEALTH



FOR: John R. Batiste, Chief



**Frank Webley**  
Contract Specialist

Signature

6-20-17

Date

5/24/17

Date

MEMORANDUM OF UNDERSTANDING

Between the

WASHINGTON STATE PATROL

And the

WASHINGTON STATE  
DEPARTMENT OF HEALTH

**I. PURPOSE**

The parties to this Memorandum of Understanding (MOU) are the Washington State Patrol, Identification and Criminal History Section (WSP) and the Washington State Department of Health, a non criminal justice agency (NCJA). This MOU sets forth the policy to ensure the protection of criminal history record information (CHRI) between the WSP, the NCJA, and the Federal Bureau of Investigation (FBI). This MOU provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CHRI data. This policy applies to the NCJA and its contractors with access to, or who operate in support of, non-criminal justice services and information.

**II. ADMINISTRATIVE RESPONSIBILITIES**

As participants in this MOU, the parties will develop mutually and separately appropriate procedures for transmission, dissemination, storage, and destruction of CHRI data.

- a. The Washington State Patrol. WSP shall ensure the NCJA complies with the Criminal Justice Information Services (CJIS) Security Policy (See Exhibit B) which includes authorized use of CHRI, dissemination of CHRI, statute authorization for civil applicant background checks conducted by noncriminal justice agencies, applicant notification and record challenge, security of CHRI, storage of CHRI, outsourcing of noncriminal justice administrative functions, and user fees. WSP will conduct regional audits of all agencies working under this MOU to ensure compliance to all state and federal standards.
- b. NCJA. The NCJA shall be responsible for ensuring:
  1. NCJA responds to requests for information by the FBI CJIS Division or the WSP in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of the agency.
  2. NCJA has formalized written procedures for the following, if applicable: criminal history use and dissemination, misuse, background checks, password management, storage, and destruction of CHRI.
  3. CHRI received as a result of licensing or employment purposes, pursuant to Public Law 92-544 is solely used for the purpose for which the record was requested. Subject fingerprints shall be submitted with all requests for CHRI for noncriminal justice purposes. Access to the FBI CJIS using name-based inquiry and record request messages is not permitted for noncriminal justice purpose, unless otherwise approved by the FBI.

4. Access to CHRI by authorized officials is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or other authorized entities.
5. All fingerprint based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.
6. NCJA must notify the applicants fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The officials making the determination of suitability for licensing or employment shall provide the applicants the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record. These officials also must advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in Title 28, C.F.R. 16.34. Official making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so.
7. Appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity.
8. NCJA shall seek WSP permission prior to outsourcing noncriminal justice functions.
9. Outsourcing of noncriminal justice administrative functions requiring access to CHRI to either another governmental agency or a private contractor acting as an agent for the authorized receiving agency complies with the security and management control outsourcing standard for non-channelers (see Exhibit A).
10. NCJA is responsible for compliance to technical standards set forth by WSP and the CJIS Security Policy.
11. NCJA will conduct periodic self audits to ensure compliance with CJIS Security Policy.
12. NCJA will participate in WSP and FBI audits, provide plans for any compliance issues, and follow through to resolution within identified timeframes.
13. NCJA will ensure all appropriate staff members are trained according to the state and federal requirements.

### **III. CRIMINAL HISTORY RECORD INFORMATION RESPONSIBILITIES**

NCJA shall conform to system policies, as established by the FBI CJIS Division and WSP, before access to CHRI is permitted. This will allow for control over the data and give assurance of system security.

1. The rules and procedures governing access to CHRI shall apply equally to all participants in the system.
2. All noncriminal justice agencies with access to CHRI data must designate a specific unit, position, or personnel to access CHRI; noncriminal justice agencies must advise WSP of such personnel and changes to such designation.
3. All noncriminal justice agencies with access to CHRI data from the system shall permit an FBI CJIS Division or WSP audit team to conduct appropriate audits. NCJA must cooperate with these audits and respond promptly.

### **IV. SECURITY RESPONSIBILITIES**

#### **Technical Roles and Responsibilities**

NCJA must comply with and enforce system security. NCJA must have someone designated as the security point of contact (POC). Security POC's shall be responsible for the following:



1. Identifying the user of the hardware/software and ensuring that no unauthorized users have access to the same.
2. Identifying and documenting how the equipment is connected to the state system.
3. Ensuring that personnel security screening procedures are being followed as stated in the CJIS Security Policy.
4. Ensuring that appropriate hardware security measures are in place.
5. Supporting policy compliance and keeping the WSP informed of security incidents.
6. If the technical POC changes at your agency, notify WSP immediately.

### **Security Enforcement**

NCJA is responsible for enforcing system security standards for their agency, in addition to all of the other agencies to which the NCJA provides CHRI information. Authorized users shall access and disseminate the CHRI data only for the purpose for which they are authorized. NCJA shall have a written policy for the discipline of policy violators.

### **Technical Security Training**

All Information Technology (IT) employees who have access to and those who have direct responsibility to configure and maintain FBI CJIS systems must review security awareness training within six months of their appointment or assignment. Documentation pertaining to the materials used and those employees which receive security awareness training shall be maintained in a current status.

### **Physical Security**

A physically secured location in a noncriminal justice facility, an area, a room, a group of rooms, that is/are subject to criminal justice agency management control security addendum and which contain hardware, software, and/or firmware (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch panels, etc.) that provide access to the CJIS sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that restrict unauthorized access.

All personnel with access to computer centers, CHRI, or areas where CHRI information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check. All personnel must review security awareness training within six months of their appointment or assignment.

### **Personnel Security**

To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days of initial employment or assignment for all personnel who have authorized access to FBI CJIS information. Those who have direct responsibility to configure and maintain computer systems and networks will not have access to FBI CJIS information. A summary of CHRI information, limited to conviction history is stored on the NCJA network; no CJIS reports are stored on the network. All emails with CJIS information attachments are printed and deleted after printing. All requests from system access shall be made as specified by the CJIS Systems Officer (i.e. WSP Identification and Criminal History Section).

- c. NCJA shall use the data supplied by WSP and the FBI under this MOU only for the authorized purpose intended. NCJA shall not use this data for any other purpose and shall not disseminate this data with any other parties unless required by law. NCJA shall share any public disclosure requests regarding this data with the WSP.

**Storage**

Please see 'Security and Management Control Outsourcing Standard for Non-Channelers' (Exhibit A).

**V. LIAISON REPRESENTATIVES  
For the Washington State Patrol:**

Jim Anderson, Administrator  
Criminal Records Division  
PO Box 42619  
Olympia WA 98504-2619  
Phone: (360) 534-2101  
Fax:(360) 534-2070  
E-mail: [jim.anderson@wsp.wa.gov](mailto:jim.anderson@wsp.wa.gov)

**For the Washington State  
Department of Health:**

T. Diane Young  
PO Box 47877  
Olympia WA 98504-7877  
360-236-4666  
[diane.young@doh.wa.gov](mailto:diane.young@doh.wa.gov)

**VI. INDEMNIFICATION**

Each party shall defend, protect and hold harmless the other party from and against all claims, suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing this MOU.

**VII. PERIOD OF MOU**

This MOU becomes effective on the date of the last signature and continues for three years and may be renewed. It may be modified by mutual written consent of the two agencies. Liaison Representatives may modify Exhibit A by mutual written consent of the two agencies without changing the general conditions of this MOU.

**VIII. TERMINATION**

Except as otherwise provided in this MOU, either party may terminate this MOU upon ninety (90) days' written notification to the other party. If this MOU is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this MOU for performance prior to the effective date of termination.

**IX. DISPUTES**

In the event that a dispute arises under this MOU, it shall be determined in the following manner: The Chief of WSP, or designee, shall appoint one member to the Dispute Board. NCJA shall appoint one member to the Dispute Board. The Chief of WSP, or designee, and the NCJA shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. If applicable and as an alternative to this process, either of the parties may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.

**X. EXHIBITS**

The exhibits listed below are incorporated into and made a part of this MOU:

Exhibit A - 'Security and Management Control Outsourcing Standard for Non-Channelers'

Exhibit B - Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.2, published 8/9/2013 which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

**XI. ORDER OF PRECEDENCE**

In the event of any inconsistency in the terms of this MOU, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

- a. Applicable federal and state statutes and regulations;
- b. The Terms and Conditions contained in this MOU;
- c. The Exhibits attached to this MOU;
- d. Any other provisions of the MOU, whether incorporated by reference or otherwise.

**XII. ALL WRITINGS CONTAINED HEREIN**

This MOU contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this MOU shall be deemed to exist or to bind any of the parties hereto.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

WASHINGTON STATE  
DEPARTMENT OF HEALTH

*for*   
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_

*8/6/14*  
\_\_\_\_\_  
Date

*07-10-14*  
\_\_\_\_\_  
Date

Dept of Health Contract #N 20392

## MEMORANDUM OF UNDERSTANDING

Between the

WASHINGTON STATE PATROL

and the

WASHINGTON STATE DEPARTMENT OF  
LABOR AND INDUSTRIES

### I. PURPOSE

The parties to this Memorandum of Understanding (MOU) are the Washington State Patrol, Identification and Criminal History Section (WSP) and the Washington State Department of Labor and Industries, a non-criminal justice agency (NCJA). This MOU sets forth the policy to ensure the protection of criminal history record information (CHRI) between the WSP, the NCJA, and the Federal Bureau of Investigation (FBI). This MOU provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CHRI data. This policy applies to the NCJA and its contractors with access to, or who operate in support of, non-criminal justice services and information.

### II. ADMINISTRATIVE RESPONSIBILITIES

As participants in this MOU, the parties will develop mutually and separately appropriate procedures for transmission, dissemination, storage, and destruction of CHRI data.

A. The Washington State Patrol. WSP shall ensure the NCJA complies with the Criminal Justice Information Services (CJIS) Security Policy (See Exhibit B) which includes authorized use of CHRI, dissemination of CHRI, statute authorization for civil applicant background checks conducted by noncriminal justice agencies, applicant notification and record challenge, security of CHRI, storage of CHRI, outsourcing of noncriminal justice administrative functions, and user fees. WSP will conduct regional audits of all agencies working under this MOU to ensure compliance to all state and federal standards.

B. NCJA. The NCJA shall be responsible for ensuring:

1. NCJA responds to requests for information by the FBI CJIS Division or the WSP in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of the agency.
2. NCJA has formalized written procedures for the following, if applicable: criminal history use and dissemination, misuse, background checks, password management, storage, and destruction of CHRI.
3. CHRI received as a result of licensing or employment purposes, pursuant to Public Law 92-544 is solely used for the purpose for which the record was requested. Subject fingerprints shall be submitted with all requests for CHRI for noncriminal justice purposes. Access to the FBI CJIS using name-based inquiry and record request messages is not permitted for noncriminal justice purpose, unless otherwise approved by the FBI.
4. Access to CHRI by authorized officials is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or other authorized entities.

5. All fingerprint based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.
6. NCJA must notify the applicants fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The officials making the determination of suitability for licensing or employment shall provide the applicants the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record. These officials also must advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in Title 28, CFR 16.34. Official making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so.
7. Appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity.
8. NCJA shall seek WSP permission prior to outsourcing noncriminal justice functions.
9. Outsourcing of noncriminal justice administrative functions requiring access to CHRI to either another governmental agency or a private contractor acting as an agent for the authorized receiving agency complies with the security and management control outsourcing standard for non-channelers (see Exhibit A).
10. NCJA is responsible for compliance to technical standards set forth by WSP and the CJIS Security Policy.
11. NCJA will conduct periodic self-audits to ensure compliance with CJIS Security Policy.
12. NCJA will participate in WSP and FBI audits, provide plans for any compliance issues, and follow through to resolution within identified timeframes.
13. NCJA will ensure all appropriate staff members are trained according to the state and federal requirements.

### **III. CRIMINAL HISTORY RECORD INFORMATION RESPONSIBILITIES**

NCJA shall conform to system policies, as established by the FBI CJIS Division and WSP, before access to CHRI is permitted. This will allow for control over the data and give assurance of system security.

1. The rules and procedures governing access to CHRI shall apply equally to all participants in the system.
2. All noncriminal justice agencies with access to CHRI data must designate a specific unit, position, or personnel to access CHRI; noncriminal justice agencies must advise WSP of such personnel and changes to such designation.
3. All noncriminal justice agencies with access to CHRI data from the system shall permit an FBI CJIS Division or WSP audit team to conduct appropriate audits. NCJA must cooperate with these audits and respond promptly.

#### IV. SECURITY RESPONSIBILITIES

##### **Technical Roles and Responsibilities**

NCJA must comply with and enforce system security. NCJA must have someone designated as the security point of contact (POC). Security POC's shall be responsible for the following:

1. Identifying the user of the hardware/software and ensuring that no unauthorized users have access to the same.
2. Identifying and documenting how the equipment is connected to the state system.
3. Ensuring that personnel security screening procedures are being followed as stated in the CJIS Security Policy.
4. Ensuring that appropriate hardware security measures are in place.
5. Supporting policy compliance and keeping the WSP informed of security incidents.
6. If the technical POC changes at your agency, notify WSP immediately.

##### **Security Enforcement**

NCJA is responsible for enforcing system security standards for their agency, in addition to all of the other agencies to which the NCJA provides CHRI information. Authorized users shall access and disseminate the CHRI data only for the purpose for which they are authorized. NCJA shall have a written policy for the discipline of policy violators.

##### **Technical Security Training**

All Information Technology (IT) employees who have access to and those who have direct responsibility to configure and maintain FBI CJIS systems must review security awareness training within six months of their appointment or assignment.

Documentation pertaining to the materials used and those employees which receive security awareness training shall be maintained in a current status.

##### **Physical Security**

A physically secured location in a noncriminal justice facility, an area, a room, a group of rooms, that is/are subject to criminal justice agency management control security addendum and which contain hardware, software, and/or firmware (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch panels, etc.) that provide access to the CJIS sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that restrict unauthorized access.

All personnel with access to computer centers, CHRI, or areas where CHRI information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check. All personnel must review security awareness training within six months of their appointment or assignment.

##### **Personnel Security**

To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days of initial employment or assignment for all personnel who have authorized access to FBI CJIS information and those who have direct responsibility to configure and maintain computer systems and networks with access to FBI CJIS information. All requests from system access shall be made as specified by the CJIS Systems Officer (i.e. WSP Identification and Criminal History Section).

NCJA shall use the data supplied by WSP and the FBI under this MOU only for the authorized purpose intended. NCJA shall not use this data for any other purpose and shall not disseminate this data with any other parties unless required by law. NCJA shall share any public disclosure requests regarding this data with the WSP.

**Storage**

Please see 'Security and Management Control Outsourcing Standard for Non-Channelers (Exhibit A).

**V. LIAISON REPRESENTATIVES**

**For the Washington State Patrol:**

Jim Anderson, Administrator  
Criminal Records Division  
PO Box 42619  
Olympia WA 98504-2619  
Phone: (360) 534-2101  
Fax:(360) 534-2070  
E-mail: jim.anderson@wsp.wa.gov

**For the Washington State Department  
of Labor and Industries:**

Ms. Jennifer Hall, Explosive Licensing  
PO Box 44655  
Tumwater WA 98504-4655  
Phone: 360-902-5563  
Email: jennifer.hall@lni.wa.gov

**VI. INDEMNIFICATION**

Each party shall defend, protect and hold harmless the other party from and against all claims, suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing this MOU.

**VII. PERIOD OF MOU**

This MOU becomes effective on the date of the last signature and continues for three years and may be renewed. It may be modified by mutual written consent of the two agencies. Liaison Representatives may modify Exhibit A by mutual written consent of the two agencies without changing the general conditions of this MOU.

**VIII. TERMINATION**

Except as otherwise provided in this MOU, either party may terminate this MOU upon ninety (90) days' written notification to the other party. If this MOU is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this MOU for performance prior to the effective date of termination.

**IX. DISPUTES**

In the event that a dispute arises under this MOU, it shall be determined in the following manner: The Chief of WSP, or designee, shall appoint one member to the Dispute Board. NCJA shall appoint one member to the Dispute Board. The Chief of WSP, or designee, and the NCJA shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. If applicable and as an alternative to this process, either of the parties may request

intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.

**X. EXHIBITS**

The exhibits listed below are incorporated into and made a part of this MOU:

Exhibit A – Security and Management Control Outsourcing Standard for Non-Channelers

Exhibit B – Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.2, published 8/9/2013 which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

Exhibit C—Additional Data Handling Requirements

**XI. ORDER OF PRECEDENCE**

In the event of any inconsistency in the terms of this MOU, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

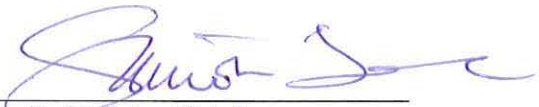
- A. Applicable federal and state statutes and regulations;
- B. The Terms and Conditions contained in this MOU;
- C. The Exhibits attached to this MOU;
- D. Any other provisions of the MOU, whether incorporated by reference or otherwise.

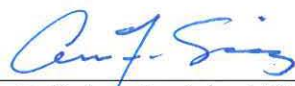
**XII. ALL WRITINGS CONTAINED HEREIN**

This MOU contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this MOU shall be deemed to exist or to bind any of the parties hereto.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

WASHINGTON STATE  
DEPARTMENT OF LABOR AND  
INDUSTRIES

*for*   
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_  
Anne F. Soiza, Assistant Director  
Division of Occupational Safety and Health

*1/22/15*  
\_\_\_\_\_  
Date

*12/23/14*  
\_\_\_\_\_  
Date



**EXHIBIT C**  
**ADDITIONAL DATA HANDLING REQUIREMENTS**

This Attachment documents the data handling requirements for transferring, accessing and protecting L&I's network and/or data shared under the terms of this Contract.

**DESCRIPTION OF DATA**

Access is granted to L&I for criminal history background information owned by Washington State Patrol. In the execution of this Contract, L&I Explosive Licensing Program submits an applicant's fingerprint card to WSP. WSP emails a password protected document (data) that contains the applicant's criminal history information. L&I reviews the information to determine if the applicant can be issued an explosives license in compliance with the RCW 70.74.360. After review of the information, the Explosives Licensing Program files the document, retains it for 6 years, and then destroys the document.

Data provided within the context of this Contract may be confidential, private and/or may contain sensitive details about an applicant's background and criminal history.

**DATA CLASSIFICATION DECLARATION**

*RCW 70.74.360 states: "(1) The director of labor and industries shall require, as a condition precedent to the original issuance and upon renewal every three years thereafter of any explosive license, fingerprinting and criminal history record information checks of every applicant. In the case of a corporation, fingerprinting and criminal history record information checks shall be required for the management officials directly responsible for the operations where explosives are used if such persons have not previously had their fingerprints recorded with the department of labor and industries. In the case of a partnership, fingerprinting and criminal history record information checks shall be required of all general partners. Such fingerprints as are required by the department of labor and industries shall be submitted on forms provided by the department to the identification section of the Washington state patrol and to the identification division of the federal bureau of investigation in order that these agencies may search their records for prior convictions of the individuals fingerprinted. The Washington state patrol shall provide to the director of labor and industries such criminal record information as the director may request. The applicant shall give full cooperation to the department of labor and industries and shall assist the department of labor and industries in all aspects of the fingerprinting and criminal history record information check. The applicant shall be required to pay the current federal and state fee for fingerprint-based criminal history background checks."*

**CHECK THE APPROPRIATE BOX**

**CONFIDENTIAL**

A data classification for data that, due to its sensitive or private nature, requires limited and authorized access. Its unauthorized access could adversely impact the agency legally, financially or damage its public integrity.

**RESTRICTED CONFIDENTIAL**

A data classification for the most sensitive medical and business data within the agency. It is Confidential (as defined above); however, with a need for added protection. Its unauthorized access would seriously and adversely impact the organization, its customers, employees or subcontractor(s).

**METHOD OF DATA ACCESS**

The data shall be provided by the Department of Labor & Industries/Information Services in the following format:

Encrypted floppy disk or CD-ROM

- Encrypted electronic-mail
- US or CMS mail
- Secure file transfer
- On-line application
- Network assessment
- Direct connection to the network –
- Other <Describe> \_\_\_\_\_

Frequency of Data Exchange

- One time: data shall be delivered by \_\_\_\_\_ (date)
- Repetitive: Each time a customer submits a fingerprint card for an Explosive License.
- As available

**AUTHORIZED ACCESS TO DATA**

Access to the data is limited to Contractor staff and subcontractor(s) who are specifically authorized and who have a business need-to-know. In accordance with the terms contained herein and prior to making the data available, the Contractor shall notify all staff and subcontractor(s) with access to the data of the use and disclosure requirements.

**USE OF DATA**

The data provided shall be used and/or accessed only for the limited purposes of carrying out activities pursuant to this Contract as described herein. The data shall not be duplicated or redisclosed without the prior written authority of L&I's Contract Manager. The Contractor shall not use the data for any purpose not specifically authorized under the terms of this Contract.

**SECURITY OF DATA**

The Contractor shall take due care to protect the data from unauthorized physical and electronic access, as described in this Contract, to ensure compliance with all appropriate federal laws and applicable provisions of Washington State law.

The handling requirements and protective measures for (Restricted) Confidential data while it is in motion and at rest are as follows:

**GENERAL ACCESS—**

Access is based on business need-to-know. It is explicitly authorized by the L&I data owner to specific individuals.

**TRANSMISSION OF DATA—**

- A) Electronic file transfer— Secure file transfer (encrypted) required.
- B) Transmission by mail—Traceable delivery required (e.g. messenger, federal or commercial courier, certified, return receipt mail).
- C) Transmission by facsimile—prohibited
- D) Electronic Mail – Encrypted email required
- E) Portable Storage Media, e.g. CDs, DVDs, USB flash drives, tapes, etc. – Encryption Required

**PRINT—**

Store in a secured, lockable enclosure.

**COPYING—**

Photocopying only with pre-authorized approval by the L&I Contract Manager. Photocopying minimized and only when necessary. Care must be taken to recover all originals and copies. Extra or spoiled copies must be disposed of properly (see Media Disposal below).

**MEDIA DISPOSAL—**

- A) Printed materials (reports and documents): Destruction is required (recycling is prohibited). Shredding or use of certified, marked and locked bins for shredding is appropriate.
  
- B) Removable magnetic or optical storage media (tape, diskettes, CDs): Media must be destroyed or deposited in certified bins specifically designated for magnetic media or "cleaned" using a U.S. Department of Defense-standard data cleaning program, and then may be reused.

**PHYSICAL SECURITY OF DATA —**

Access to areas containing the data must be physically restricted. Data must be locked when left unattended.

**ELECTRONIC DATA AT REST—**

If there is a need for data to be stored on a PC, the Contractor must assure unauthorized access cannot take place, including but not limited to password protection when PC is left unattended. Data stored on non-L&I equipment must be encrypted.

**AUTHENTICATION OF USER IDENTITY—**

- 1. Authentication from inside an L&I facility for Contractor staff to access internal LAN and computer systems—requires user ID and password
  
- 2. Authentication for Contractor staff from a location outside of an L&I facility—strong authentication (e.g., digital certificates, hardware, tokens, biometrics, etc) is required.

**DATA RECOVERY—**

Loss of the data or equipment – Legal notification to L&I's contract manager is required.

**DATA DISPOSITION (MEDIA DISPOSAL)—**

Upon completion of work, the data collected must be destroyed or returned to L&I. Certification of Data Disposition form (Attachment F) is required.

**SYSTEMS MANAGEMENT—**

Contractor shall ensure all systems, including portable systems are maintained with all best security practices including but not limited to up-to-date anti-virus protection, security patches, firewall(s), full disk encryption, etc.

**TERMINATION OF ACCESS**

Each party may at its discretion disqualify an individual authorized by the other party from gaining access to data. Notice of termination of access will be by written notice and become effective upon receipt by the other party. Termination of access of one individual by either party does not affect other individuals authorized under this Agreement.

**Amendment Summary**

**Contract Number** C130698GSC-1  
**Contract Office Consultant** Rebecca Kirby  
**Contract Manager** Deb Collinsworth  
**Created Date** 10/18/2017

Vendor Information

**Vendor Number** SWW0014152-16  
**Legal Name** WA State Labor & Industries  
**DBA Name** Washington State Department of Labor & Industries  
**UBI Number**  
**Address** PO BOX 44655, Olympia, WA USA 98504 -4655

Contract Information

**Short Description** Security of CHRI  
**Competition Method(s)** None  
**Master Index Code(s)** o 000ID240 - Identification Section (2015)  
**Organization Index Code**  
**Program Code** 020 (Investigative Services Bureau)  
**Subprogram Code** 03 (Criminal Records Division)  
**Object Sub Sub/Object(s)** CZ (Other Professional Services)  
**Contract Purpose** Security of CHRI

| Dates          | Start Date | End Date   |
|----------------|------------|------------|
| Original       | 01/12/2015 | 01/11/2018 |
| This Amendment | 01/12/2015 | 01/11/2023 |
| Current        | 01/12/2015 | 01/11/2023 |

**Solicitation Number(s)**  
**Expenditure Type(s)** Non-Financial (NFC)  
**Authority** Interagency Agreements (RCW 39.34)  
**Vendor Type** Public Agency

| Contract Reference Number(s) | Reference Number |
|------------------------------|------------------|
|                              | Internal         |
| K3228                        | External         |

**Funding Source(s)**  
**Prior Total** \$0.00  
**Federal Funds**  
**State Funds**  
**Other Funds**  
**Sub Total** NFC

**Current Contract Total** NFC  
**Contract Remaining Balance** NFC

**Performance-based contracting (PBC)** The contract for this amendment is performance-based.

*Sent to vendor for sig. 10/19/2017  
 Sent revised contract to vendor  
 Sent exe. copy to vendor 2/16/2018 1/16/2018  
 Dist. exe. copy 2/16/2018*

Contact Information

Rebecca Kirby

Rebecca.kirby@wsp.wa.gov

Deb Collinsworth

Deborah.Collinsworth@wsp.wa.gov

**Miscellaneous**

**Notes**

**Custom Fields - Contract Tracking Information**

**Contract Sent to Contractor**      01/15/2015

**Custom Fields - Agreement Type**

**Agreement Type**                      • Memorandum of Understanding (MOU)

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

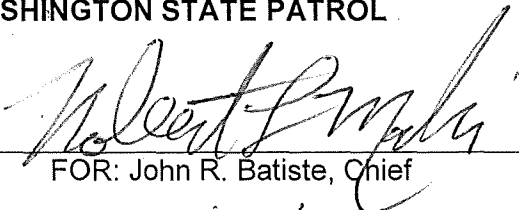
The above referenced Contract between the Washington State Patrol and the Washington State Department of Labor and Industries is hereby amended as follows:

- The end date shall be extended through January 11, 2023.
- Section V, Liaison Representatives with the following:  
Mr. Daniel Massey, Explosive Licensing  
PO Box 44655  
Tumwater WA 98504-4655  
Ph. 360-902-5569  
[Daniel.massey@lni.wa.gov](mailto:Daniel.massey@lni.wa.gov)
- **Exhibit B** "CJIS Security Policy" shall be replaced by **Exhibit B** – Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.6, published 6/5/2017 which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.
- **Exhibit C** "Additional Data Handling Requirements"

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

  
FOR: John R. Batiste, Chief

2/15/18  
Date

WASHINGTON STATE DEPARTMENT OF  
LABOR AND INDUSTRIES

  
Signature

2/13/2018  
Date

**EXHIBIT C**  
**ADDITIONAL DATA HANDLING REQUIREMENTS**

This Attachment documents the data handling requirements for transferring, accessing and protecting L&I's network and/or data shared under the terms of this Contract.

**DESCRIPTION OF DATA**

Access is granted to L&I for criminal history background information owned by Washington State Patrol. In the execution of this Contract, L&I Explosive Licensing Program submits an applicant's fingerprint card to WSP. WSP emails a password protected document (data) that contains the applicant's criminal history information. L&I reviews the information to determine if the applicant can be issued an explosives license in compliance with the RCW 70.74.360. After review of the information, the Explosives Licensing Program files the document, retains it for the period specified by the Secretary of State Disposition Authorization Number (DAN) 87-10-41113, and then destroys the document.

Data provided within the context of this Contract may be confidential, private and/or may contain sensitive details about an applicant's background and criminal history.

**DATA CLASSIFICATION DECLARATION**

*RCW 70.74.360 states: "(1) The director of labor and industries shall require, as a condition precedent to the original issuance and upon renewal every three years thereafter of any explosive license, fingerprinting and criminal history record information checks of every applicant. In the case of a corporation, fingerprinting and criminal history record information checks shall be required for the management officials directly responsible for the operations where explosives are used if such persons have not previously had their fingerprints recorded with the department of labor and industries. In the case of a partnership, fingerprinting and criminal history record information checks shall be required of all general partners. Such fingerprints as are required by the department of labor and industries shall be submitted on forms provided by the department to the identification section of the Washington state patrol and to the identification division of the federal bureau of investigation in order that these agencies may search their records for prior convictions of the individuals fingerprinted. The Washington state patrol shall provide to the director of labor and industries such criminal record information as the director may request. The applicant shall give full cooperation to the department of labor and industries and shall assist the department of labor and industries in all aspects of the fingerprinting and criminal history record information check. The applicant shall be required to pay the current federal and state fee for fingerprint-based criminal history background checks."*

CHECK THE APPROPRIATE BOX

CONFIDENTIAL

A data classification for data that, due to its sensitive or private nature, requires limited and authorized access. Its unauthorized access could adversely impact the agency legally, financially or damage its public integrity.

RESTRICTED CONFIDENTIAL

A data classification for the most sensitive medical and business data within the agency.. It is Confidential (as defined above); however, with a need for added protection. Its unauthorized access would seriously and adversely impact the organization, its customers, employees or subcontractor(s).

**METHOD OF DATA ACCESS**

The data shall be provided by the Department of Labor & Industries/Information Services in the following format:

- Encrypted floppy disk or CD-ROM
- Encrypted electronic-mail
- US or CMS mail
- Secure file transfer
- On-line application
- Network assessment
- Direct connection to the network –
- Other <Describe> \_\_\_\_\_

Frequency of Data Exchange

- One time: data shall be delivered by \_\_\_\_\_ (date)
- Repetitive: Each time a customer submits a fingerprint card for an Explosive License.
- As available

**AUTHORIZED ACCESS TO DATA**

Access to the data is limited to Contractor staff and subcontractor(s) who are specifically authorized and who have a business need-to-know. In accordance with the terms contained herein and prior to making the data available, the Contractor shall notify all staff and subcontractor(s) with access to the data of the use and disclosure requirements.

**USE OF DATA**

The data provided shall be used and/or accessed only for the limited purposes of carrying out activities pursuant to this Contract as described herein. The data shall not be duplicated or redisclosed without the prior written authority of L&I's Contract Manager. The Contractor shall not use the data for any purpose not specifically authorized under the terms of this Contract.

**SECURITY OF DATA**

The Contractor shall take due care to protect the data from unauthorized physical and electronic access, as described in this Contract, to ensure compliance with all appropriate federal laws and applicable provisions of Washington State law.

The handling requirements and protective measures for (Restricted) Confidential data while it is in motion and at rest are as follows:

**GENERAL ACCESS—**

Access is based on business need-to-know. It is explicitly authorized by the L&I data owner to specific individuals.

**TRANSMISSION OF DATA—**

- A) Electronic file transfer— Secure file transfer (encrypted) required.
- B) Transmission by mail—Traceable delivery required (e.g. messenger, federal or commercial courier, certified, return receipt mail).
- C) Transmission by facsimile—prohibited
- D) Electronic Mail – Encrypted email required
- E) Portable Storage Media, e.g. CDs, DVDs, USB flash drives, tapes, etc. – Encryption Required

**PRINT—**

Store in a secured, lockable enclosure.



**COPYING—**

Photocopying only with pre-authorized approval by the L&I Contract Manager. Photocopying minimized and only when necessary. Care must be taken to recover all originals and copies. Extra or spoiled copies must be disposed of properly (see Media Disposal below).

**MEDIA DISPOSAL—**

- A) Printed materials (reports and documents): Destruction is required (recycling is prohibited). Shredding or use of certified, marked and locked bins for shredding is appropriate.
- B) Removable magnetic or optical storage media (tape, diskettes, CDs): Media must be destroyed or deposited in certified bins specifically designated for magnetic media or "cleaned" using a U.S. Department of Defense-standard data cleaning program, and then may be reused.

**PHYSICAL SECURITY OF DATA —**

Access to areas containing the data must be physically restricted. Data must be locked when left unattended.

**ELECTRONIC DATA AT REST—**

If there is a need for data to be stored on a PC, the Contractor must assure unauthorized access cannot take place, including but not limited to password protection when PC is left unattended. Data stored on non-L&I equipment must be encrypted.

**AUTHENTICATION OF USER IDENTITY—**

- 1. Authentication from inside an L&I facility for Contractor staff to access internal LAN and computer systems—requires user ID and password
- 2. Authentication for Contractor staff from a location outside of an L&I facility—strong authentication (e.g., digital certificates, hardware, tokens, biometrics, etc) is required.

**DATA RECOVERY—**

Loss of the data or equipment – Legal notification to L&I's contract manager is required.

**DATA DISPOSITION (MEDIA DISPOSAL)—**

Upon completion of work, the data collected must be destroyed or returned to L&I. Certification of Data Disposition form (Attachment F) is required.

**SYSTEMS MANAGEMENT—**

Contractor shall ensure all systems, including portable systems are maintained with all best security practices including but not limited to up-to-date anti-virus protection, security patches, firewall(s), full disk encryption, etc.

**TERMINATION OF ACCESS**

Each party may at its discretion disqualify an individual authorized by the other party from gaining access to data. Notice of termination of access will be by written notice and become effective upon receipt by the other party. Termination of access of one individual by either party does not affect other individuals authorized under this Agreement.

**MEMORANDUM OF UNDERSTANDING**

**Between the**

**WASHINGTON STATE PATROL**

**And the**

**WASHINGTON OFFICE  
OF THE INSURANCE COMMISSIONER**

**I. PURPOSE**

The parties to this Memorandum of Understanding (MOU) are the Washington State Patrol, Identification and Criminal History Section (WSP) and the Washington State Office of the Insurance Commissioner, a non criminal justice agency (NCJA). This MOU sets forth the policy to ensure the protection of criminal history record information (CHRI) between the WSP, the NCJA, and the Federal Bureau of Investigation (FBI). This MOU provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CHRI data. This policy applies to the NCJA and its contractors with access to, or who operate in support of, non-criminal justice services and information.

**II. ADMINISTRATIVE RESPONSIBILITIES**

As participants in this MOU, the parties will develop mutually and separately appropriate procedures for transmission, dissemination, storage, and destruction of CHRI data.

a. The Washington State Patrol. WSP shall ensure the NCJA complies with the Criminal Justice Information Services (CJIS) Security Policy (See Exhibit B) which includes authorized use of CHRI, dissemination of CHRI, statute authorization for civil applicant background checks conducted by noncriminal justice agencies, applicant notification and record challenge, security of CHRI, storage of CHRI, outsourcing of noncriminal justice administrative functions, and user fees. WSP will conduct regional audits of all agencies working under this MOU to ensure compliance to all state and federal standards.

b. NCJA. The NCJA shall be responsible for ensuring:

1. NCJA responds to requests for information by the FBI CJIS Division or the WSP in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of the agency.
2. NCJA has formalized written procedures for the following, if applicable: criminal history use and dissemination, misuse, background checks, password management, storage, and destruction of CHRI.
3. CHRI received as a result of licensing or employment purposes, pursuant to Public Law 92-544 is solely used for the purpose for which the record was requested. Subject fingerprints shall be submitted with all requests for CHRI for noncriminal justice purposes. Access to the FBI CJIS using name-based inquiry and record request messages is not permitted for noncriminal justice purpose, unless otherwise approved by the FBI.

4. Access to CHRI by authorized officials is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or other authorized entities.
5. All fingerprint based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.
6. NCJA must notify the applicants fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The officials making the determination of suitability for licensing or employment shall provide the applicants the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record. These officials also must advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in Title 28, C.F.R. 16.34. Official making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so.
7. Appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity.
8. NCJA shall seek WSP permission prior to outsourcing noncriminal justice functions.
9. Outsourcing of noncriminal justice administrative functions requiring access to CHRI to either another governmental agency or a private contractor acting as an agent for the authorized receiving agency complies with the security and management control outsourcing standard for non-channelers (see Exhibit A).
10. NCJA is responsible for compliance to technical standards set forth by WSP and the CJIS Security Policy.
11. NCJA will conduct periodic self audits to ensure compliance with CJIS Security Policy.
12. NCJA will participate in WSP and FBI audits, provide plans for any compliance issues, and follow through to resolution within identified timeframes.
13. NCJA will ensure all appropriate staff members are trained according to the state and federal requirements.

### **III. CRIMINAL HISTORY RECORD INFORMATION RESPONSIBILITIES**

NCJA shall conform to system policies, as established by the FBI CJIS Division and WSP, before access to CHRI is permitted. This will allow for control over the data and give assurance of system security.

1. The rules and procedures governing access to CHRI shall apply equally to all participants in the system.
2. All noncriminal justice agencies with access to CHRI data must designate a specific unit, position, or personnel to access CHRI; noncriminal justice agencies must advise WSP of such personnel and changes to such designation.
3. All noncriminal justice agencies with access to CHRI data from the system shall permit an FBI CJIS Division or WSP audit team to conduct appropriate audits. NCJA must cooperate with these audits and respond promptly.

### **IV. SECURITY RESPONSIBILITIES**

#### **Technical Roles and Responsibilities**

NCJA must comply with and enforce system security. NCJA must have someone designated as the security point of contact (POC). Security POC's shall be responsible for the following:

1. Identifying the user of the hardware/software and ensuring that no unauthorized users have access to the same.
2. Identifying and documenting how the equipment is connected to the state system.
3. Ensuring that personnel security screening procedures are being followed as stated in the CJIS Security Policy.
4. Ensuring that appropriate hardware security measures are in place.
5. Supporting policy compliance and keeping the WSP informed of security incidents.
6. If the technical POC changes at your agency, notify WSP immediately.

#### **Security Enforcement**

NCJA is responsible for enforcing system security standards for their agency, in addition to all of the other agencies to which the NCJA provides CHRI information. Authorized users shall access and disseminate the CHRI data only for the purpose for which they are authorized. NCJA shall have a written policy for the discipline of policy violators.

#### **Technical Security Training**

All Information Technology (IT) employees who have access to and those who have direct responsibility to configure and maintain FBI CJIS systems must review security awareness training within six months of their appointment or assignment. Documentation pertaining to the materials used and those employees which receive security awareness training shall be maintained in a current status.

#### **Physical Security**

A physically secured location in a noncriminal justice facility, an area, a room, a group of rooms, that is/are subject to criminal justice agency management control security addendum and which contain hardware, software, and/or firmware (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch panels, etc.) that provide access to the CJIS sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that restrict unauthorized access.

All personnel with access to computer centers, CHRI, or areas where CHRI information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check. All personnel must review security awareness training within six months of their appointment or assignment.

#### **Personnel Security**

To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days of initial employment or assignment for all personnel who have authorized access to FBI CJIS information and those who have direct responsibility to configure and maintain computer systems and networks with access to FBI CJIS information. All requests from system access shall be made as specified by the CJIS Systems Officer (i.e. WSP Identification and Criminal History Section).

- c. NCJA shall use the data supplied by WSP and the FBI under this MOU only for the authorized purpose intended. NCJA shall not use this data for any other purpose and shall not disseminate this data with any other parties unless required by law. NCJA shall share any public disclosure requests regarding this data with the WSP.

**Storage**

Please see 'Security and Management Control Outsourcing Standard for Non-Channelers' (Exhibit A).

**V. LIAISON REPRESENTATIVES**

**For the Washington State Patrol:**

Jim Anderson, Administrator  
Criminal Records Division  
PO Box 42619  
Olympia WA 98504-2619  
Phone: (360) 534-2101  
Fax:(360) 534-2070  
E-mail: [jim.anderson@wsp.wa.gov](mailto:jim.anderson@wsp.wa.gov)

**For the Washington Office  
of the Insurance Commissioner:**

Jeff Baughman  
PO Box 40257  
Olympia WA 98504  
360-725-7064  
JeffB@oic.wa.gov

**VI. INDEMNIFICATION**

Each party shall defend, protect and hold harmless the other party from and against all claims, suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing this MOU.

**VII. PERIOD OF MOU**

This MOU becomes effective on the date of the last signature and continues for three years and may be renewed. It may be modified by mutual written consent of the two agencies. Liaison Representatives may modify Exhibit A by mutual written consent of the two agencies without changing the general conditions of this MOU.

**VIII. TERMINATION**

Except as otherwise provided in this MOU, either party may terminate this MOU upon ninety (90) days' written notification to the other party. If this MOU is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this MOU for performance prior to the effective date of termination.

**IX. DISPUTES**

In the event that a dispute arises under this MOU, it shall be determined in the following manner: The Chief of WSP, or designee, shall appoint one member to the Dispute Board. NCJA shall appoint one member to the Dispute Board. The Chief of WSP, or designee, and the NCJA shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. If applicable and as an alternative to this process, either of the parties may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.

**X. EXHIBITS**

The exhibits listed below are incorporated into and made a part of this MOU:

Exhibit A - 'Security and Management Control Outsourcing Standard for Non-Channelers'

Exhibit B - Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.2, published 8/9/2013 which is available at the following link:

[www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

**XI. ORDER OF PRECEDENCE**

In the event of any inconsistency in the terms of this MOU, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

- a. Applicable federal and state statutes and regulations;
- b. The Terms and Conditions contained in this MOU;
- c. The Exhibits attached to this MOU;
- d. Any other provisions of the MOU, whether incorporated by reference or otherwise.

**XII. ALL WRITINGS CONTAINED HEREIN**

This MOU contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this MOU shall be deemed to exist or to bind any of the parties hereto.

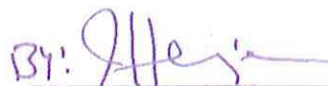
STATE OF WASHINGTON  
WASHINGTON STATE PATROL

  
\_\_\_\_\_  
John R. Batiste, Chief

Date

3/13/14

WASHINGTON OFFICE  
OF THE INSURANCE COMMISSIONER

BY:   
\_\_\_\_\_  
J. HAMJE, DEP. INS. COMMISSIONER

Date

3-12-2014

[www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

**XI. ORDER OF PRECEDENCE**

In the event of any inconsistency in the terms of this MOU, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

- a. Applicable federal and state statutes and regulations;
- b. The Terms and Conditions contained in this MOU;
- c. The Exhibits attached to this MOU;
- d. Any other provisions of the MOU, whether incorporated by reference or otherwise.

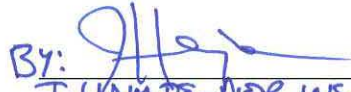
**XII. ALL WRITINGS CONTAINED HEREIN**

This MOU contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this MOU shall be deemed to exist or to bind any of the parties hereto.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

WASHINGTON OFFICE  
OF THE INSURANCE COMMISSIONER

\_\_\_\_\_  
John R. Batiste, Chief

By:   
J. HAMJE, DEP. INS. COMMISSIONER

\_\_\_\_\_  
Date

3-12-2014  
\_\_\_\_\_  
Date

## SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD for NON-CHANNELERS

The goal of this document is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the Contractor. Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security and Management Control Outsourcing Standard (Outsourcing Standard) is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI without a direct connection to the FBI CJIS Wide Area Network (WAN).

### 1.0 Definitions

- 1.01 *Access to CHRI* means to view or make use of CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by title 42, United States Code, section 14614(b).
- 1.02 *Authorized Recipient* means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.
- 1.03 *Chief Administrator* means the primary administrator of a Nonparty State’s criminal history record repository or a designee of such administrator who is



a regular full-time employee of the repository, which is also referred to as the State Identification Bureau (SIB) Chief.

- 1.04 *CHRI*, as referred to in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.
- 1.05 *Criminal History Record Check*, for purposes of this Outsourcing Standard only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.
- 1.06 *Compact Officer*, as provided in Article I(2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the compact among federal agencies], or (B) with respect to a Party State, the chief administrator of the State's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.
- 1.07 *Contractor* means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI.
- 1.08 *Dissemination* means the disclosure of III CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 1.09 *Noncriminal Justice Administrative Functions* means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:
1. Making fitness determinations/recommendations
  2. Obtaining missing dispositions
  3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General
  4. Other authorized activities relating to the general handling, use, and storage of CHRI

- 1.10 *Noncriminal Justice Purposes*, as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.
- 1.11 *Outsourcing Standard* means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. This Outsourcing Standard authorizes access to CHRI for noncriminal justice purposes, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.
- 1.12 *Physically Secure Location* means a facility or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CHRI and associated information systems.
- 1.13 *Positive Identification*, as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints<sup>1</sup> or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other non-unique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.
- 1.14 *Public Carrier Network* means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: Dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.
- 1.15 *Security Violation* means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in

---

<sup>1</sup> The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning positive identification may be obtained from the FBI Compact Council office.

violation of: (A) Federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

2.0 *Responsibilities of the Authorized Recipient*

- 2.01 Prior to engaging in outsourcing any noncriminal justice administrative functions, the Authorized Recipient shall: (a) Request and receive written permission from (1) the State Compact Officer/Chief Administrator<sup>2</sup> or (2) the FBI Compact Officer<sup>3</sup>; (b) provide the Compact Officer/Chief Administrator copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested; and (c) inquire of the FBI Compact Officer whether a prospective Contractor has any security violations (See Section 8.04). The FBI Compact Officer will report those findings to the Authorized Recipient and, when applicable, to the State Compact Officer/Chief Administrator.
- 2.02 The Authorized Recipient shall execute a contract or agreement prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.
- 2.03 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; limit retention of the information to a period of time not to exceed that period of time the Authorized Recipient is permitted to retain such information; prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General; ensure the security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; and ensure that Contractor

---

<sup>2</sup>The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and Authorized Recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.

<sup>3</sup>State or local Authorized Recipients based on State or Federal Statutes shall contact the State Compact Officer/Chief Administrator. Federal or Regulatory Agency Authorized Recipients shall contact the FBI Compact Officer.

personnel comply with this Outsourcing Standard.

- a. The Authorized Recipient shall conduct criminal history record checks of Contractor personnel having access to CHRI if such checks are required or authorized of the Authorized Recipient's personnel having similar access.<sup>4</sup> The Authorized Recipient shall maintain updated records of Contractor personnel who have access to CHRI and update those records within 24 hours when changes to that access occur and, if a criminal history record check is required, the Authorized Recipient shall maintain a list of Contractor personnel who successfully completed the criminal history record check.
  - b. The Authorized Recipient shall ensure that the Contractor maintains site security.
  - c. The Authorized Recipient shall ensure that the most current version of both the Outsourcing Standard and the CJIS Security Policy are incorporated by reference at the time of contract, contract renewal, or within 30 calendar days (unless otherwise directed) of notification of successor versions of the Outsourcing Standard and/or CJIS Security Policy, whichever is sooner. The Authorized Recipient shall notify the Contractor within 30 calendar days (unless otherwise directed) of FBI notification regarding changes or updates to the Outsourcing Standard and/or CJIS Security Policy.
- 2.04 The Authorized Recipient shall understand the communications and record capabilities of the Contractor which has access to federal or state records through, or because of, its outsourcing relationship with the Authorized Recipient. The Authorized Recipient shall maintain an updated topological drawing which depicts the interconnectivity of the Contractor's network configuration.
- 2.05 The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the Outsourcing Standard. The Authorized Recipient shall certify to the Compact Officer/Chief Administrator that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.

---

<sup>4</sup>If a national criminal history record check of Authorized Recipient personnel having access to CHRI is mandated or authorized by a federal statute, executive order, or state statute approved by the Attorney General under Public Law 92-544, the State Compact Officer/Chief Administrator and/or the FBI Compact Officer must ensure Contractor personnel having similar access are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives. The national criminal history record checks of Contractor personnel with access to CHRI cannot be outsourced and must be performed by the Authorized Recipient.

2.06 The Authorized Recipient shall provide written notice of any early voluntary termination of the contract to the Compact Officer/Chief Administrator or the FBI Compact Officer.

3.0 *Responsibilities of the Contractor*

3.01 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the CJIS Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

3.02 The Contractor shall develop, document, administer, and maintain a Security Program (Physical, Personnel, and Information Technology) to comply with the most current Outsourcing Standard and the most current FBI *CJIS Security Policy*. The Security Program shall describe the implementation of the security requirements described in this Outsourcing Standard and the FBI *CJIS Security Policy*. In addition, the Contractor is also responsible to set, maintain, and enforce the standards for the selection, supervision, and separation of personnel who have access to CHRI. The Authorized Recipient shall provide the written approval of a Contractor's Security Program.

3.03 The requirements for a Security Program should include, at a minimum:

- a) Description of the implementation of the security requirements described in this Outsourcing Standard and the *CJIS Security Policy*.
- b) Security Training.
- c) Guidelines for documentation of security violations.
- d) Standards for the selection, supervision, and separation of personnel with access to CHRI.

\*\*If the Contractor is using a corporate policy, it must meet the requirements outlined in this Outsourcing Standard and the *CJIS Security Policy*. If the corporate policy is not this specific, it must flow down to a level where the documentation supports these requirements.

3.04 Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. The Authorized Recipient shall review and provide to the Contractor written approval of the Security Training Program. Training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall annually, not later than the anniversary date of the contract, certify in writing to the Authorized Recipient that annual refresher training was completed for those Contractor personnel with access

to CHRI.

- 3.05 The Contractor shall make its facilities available for announced and unannounced audits performed by the Authorized Recipient, the state, or the FBI on behalf of the Compact Council.
- 3.06 The Contractor's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI CJIS Division. During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.
- 3.07 The Contractor shall maintain CHRI only for the period of time necessary to fulfill its contractual obligations but not to exceed the period of time that the Authorized Recipient is authorized to maintain and does maintain the CHRI.
- 3.08 The Contractor shall maintain a log of any dissemination of CHRI, for a minimum of 365 days.

#### 4.0 *Site Security*

- 4.01 The Authorized Recipient shall ensure that the Contractor site(s) is a physically secure location to protect against any unauthorized access to CHRI.

#### 5.0 *Dissemination*

- 5.01 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 5.02 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) The Authorized Recipient and the secondary recipient with unique identifiers, (B) the record disseminated, (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.
- 5.03 If CHRI is stored or disseminated in an electronic format, the Contractor shall protect against unauthorized access to the equipment and any of the data. In no event shall responses containing CHRI be disseminated other than as governed by this Outsourcing Standard or more stringent contract requirements.

#### 6.0 *Personnel Security*

- 6.01 If a local, state, or federal written standard requires or authorizes a criminal history record check of the Authorized Recipient's personnel with access to

CHRI, then a criminal history record check shall be required of the Contractor's (and approved Sub-Contractor's) employees having access to CHRI. Criminal history record checks of Contractor and approved Sub-Contractor employees, at a minimum, will be no less stringent than criminal history record checks that are performed on the Authorized Recipient's personnel performing similar functions. Criminal history record checks must be completed prior to accessing CHRI under the contract.

- 6.02 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm in writing that each employee has certified in writing that he/she understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities. The Contractor shall maintain the employee certifications in a file that is subject to review during audits. Employees shall make such certification prior to performing work under the contract.
- 6.03 The Contractor shall maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur, and if a criminal history record check is required, maintain a list of personnel who have successfully completed criminal history record checks. The Contractor shall notify Authorized Recipients within 24 hours when additions or deletions occur.

## 7.0 *System Security*

- 7.01 The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy.
  - a. If CHRI can be accessed by unauthorized personnel via Wide Area Network/Local Area Network or the Internet, then the Contractor shall protect the CHRI with firewall-type devices to prevent such unauthorized access. These devices shall implement a minimum firewall profile as specified by the CJIS Security Policy in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.
  - b. Data encryption shall be required throughout the network passing CHRI through a shared public carrier network.
- 7.02 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.
  - a. CHRI shall be stored in a physically secure location.
  - b. The Authorized Recipient shall ensure that a procedure is in place for

sanitizing all fixed storage media (e.g., disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal, or reuse. Sanitization procedures include overwriting the media and/or degaussing the media.

- c. The Authorized Recipient shall ensure that a procedure is in place for the disposal or return of all non-fixed storage media (e.g., hard copies, print-outs).
- 7.03 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient, Contractor, or sub-Contractor must be assigned a unique identifying number.

## 8.0 *Security Violations*

### 8.01 Duties of the Authorized Recipient and Contractor

- a. The Contractor shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference.
- b. Pending investigation, the Contractor shall, upon detection or awareness, suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.
- c. The Contractor shall immediately (within four hours) notify the Authorized Recipient of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. Within five calendar days of such notification, the Contractor shall provide the Authorized Recipient a written report documenting such security violation, any corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.
- d. The Authorized Recipient shall immediately (within four hours) notify the State Compact Officer/Chief Administrator and the FBI Compact Officer of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator, if applicable, and the FBI Compact Officer, within five calendar days of receipt of the written report from the Contractor. The written report must include any corrective actions taken by the Contractor and the Authorized Recipient to resolve such security violation.



- 8.02 Termination of the contract by the Authorized Recipient for security violations
- a. The contract is subject to termination by the Authorized Recipient for security violations involving CHRI obtained pursuant to the contract.
  - b. The contract is subject to termination by the Authorized Recipient for the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.
  - c. If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient shall terminate the contract.
- 8.03 Suspension or termination of the exchange of CHRI for security violations
- a. Notwithstanding the actions taken by the State Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Compact Council or the United States Attorney General may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 CFR §906.2(d).
  - b. If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United States Attorney General by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be deleted or returned in accordance with the provisions and time frame as specified by the Authorized Recipient.
- 8.04 The Authorized Recipient shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following:
- a. The termination of a contract for security violations.
  - b. Security violations involving the unauthorized access to CHRI.
  - c. The Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.
- 8.05 The Compact Officer/Chief Administrator, Compact Council and the United States Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.
- 8.06 The Compact Officer/Chief Administrator, Compact Council, and the United

States Attorney General reserve the right to audit the Authorized Recipient and the Contractor's operations and procedures at scheduled or unscheduled times. The Compact Council, the United States Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the contract.

#### 9.0 *Miscellaneous Provisions*

- 9.01 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, Compact Officer/Chief Administrator (where applicable), and the FBI.
- 9.02 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) The CJIS Security Policy.
- 9.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and the CHRI accessed therefrom and it is understood that there may be terms and conditions of the appended contract which impose more stringent requirements upon the Contractor.<sup>5</sup>
- 9.04 The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. Conformance to such security measures may not be less stringent than stated in this Outsourcing Standard without the consent of the Compact Council in consultation with the United States Attorney General.
- 9.05 This Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.
- 9.06 Appropriate notices, assurances, and correspondence to the FBI Compact Officer, Compact Council, and the United States Attorney General required by Section 8.0 of this Outsourcing Standard shall be forwarded by First Class Mail to:

FBI Compact Officer  
1000 Custer Hollow Road  
Module D-3  
Clarksburg, WV 26306

#### 10.0 *Exemption from Above Provisions*

---

<sup>5</sup>Such conditions could include additional audits, fees, or security requirements. The Compact Council, Authorized Recipients, and the Compact Officer/Chief Administrator have the explicit authority to require more stringent standards than those contained in the Outsourcing Standard.

- 10.01 An Information Technology (IT) contract need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:
1. Access to CHRI by the IT contractor's personnel is limited solely for the development and/or maintenance of the Authorized Recipient's computer system;
  2. Access to CHRI is incidental, but necessary, to the duties being performed by the IT contractor;
  3. The computer system resides within the Authorized Recipient's facility;
  4. The Authorized Recipient's personnel supervise or work directly with the IT contractor personnel;
  5. The Authorized Recipient maintains complete, positive control of the IT contractor's access to the computer system and CHRI contained therein; and
  6. The Authorized Recipient retains all of the duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard.

10.02 An Authorized Recipient's contract where access to CHRI is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 4.0, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:

1. Access to CHRI by the Contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient;
2. Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor;

3. The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the Authorized Recipient;
4. The Contractor's personnel are subject to the same criminal history record checks as the Authorized Recipient's personnel;
5. The criminal history record checks of the Contractor personnel are completed prior to work on the contract or agreement;
6. The Authorized Recipient retains all other duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard; and
7. The Contractor stores the CHRI in a physically secure location.

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above referenced Contract between the Washington State Patrol and the Washington Office of the Insurance Commissioner is hereby amended as follows:

- The end date shall be extended through March 12, 2022.
- **Exhibit B** "CJIS Security Policy" shall be replaced by **Exhibit B** – Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.5, published 6/1/2016 which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

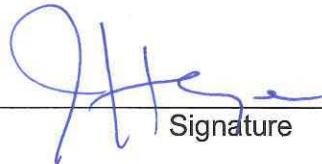
STATE OF WASHINGTON  
WASHINGTON STATE PATROL



FOR: John R. Batiste, Chief

3/31/2017  
Date

WASHINGTON OFFICE OF THE  
INSURANCE COMMISSIONER



Signature

3-28-2017  
Date

**MEMORANDUM OF UNDERSTANDING**

Between the

**WASHINGTON STATE PATROL**

And the

**WASHINGTON STATE  
INVESTMENT BOARD**

**I. PURPOSE**

The parties to this Memorandum of Understanding (MOU) are the Washington State Patrol, Identification and Criminal History Section (WSP) and the Washington State Investment Board, a non criminal justice agency (NCJA). This MOU sets forth the policy to ensure the protection of criminal history record information (CHRI) between the WSP, the NCJA, and the Federal Bureau of Investigation (FBI). This MOU provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CHRI data. This policy applies to the NCJA and its contractors with access to, or who operate in support of, non-criminal justice services and information.

**II. ADMINISTRATIVE RESPONSIBILITIES**

As participants in this MOU, the parties will develop mutually and separately appropriate procedures for transmission, dissemination, storage, and destruction of CHRI data.

ee. The Washington State Patrol. WSP shall ensure the NCJA complies with the Criminal Justice Information Services (CJIS) Security Policy (See Exhibit B) which includes authorized use of CHRI, dissemination of CHRI, statute authorization for civil applicant background checks conducted by noncriminal justice agencies, applicant notification and record challenge, security of CHRI, storage of CHRI, outsourcing of noncriminal justice administrative functions, and user fees. WSP will conduct regional audits of all agencies working under this MOU to ensure compliance to all state and federal standards.

ff. NCJA. The NCJA shall be responsible for ensuring:

131. NCJA responds to requests for information by the FBI CJIS Division or the WSP in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of the agency.

132. NCJA has formalized written procedures for the following, if applicable: criminal history use and dissemination, misuse, background checks, password management, storage, and destruction of CHRI.

133. CHRI received as a result of licensing or employment purposes, pursuant to Public Law 92-544 is solely used for the purpose for which the record was requested. Subject fingerprints shall be submitted with all requests for CHRI for noncriminal justice purposes. Access to the FBI CJIS using name-based inquiry and record request messages is not permitted for noncriminal justice purpose, unless otherwise approved by the FBI.

134. Access to CHRI by authorized officials is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or other authorized entities.

135. All fingerprint based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.
136. NCJA must notify the applicants fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The officials making the determination of suitability for licensing or employment shall provide the applicants the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record. These officials also must advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in Title 28, C.F.R. 16.34. Official making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so.
137. Appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity.
138. NCJA shall seek WSP permission prior to outsourcing noncriminal justice functions.
139. Outsourcing of noncriminal justice administrative functions requiring access to CHRI to either another governmental agency or a private contractor acting as an agent for the authorized receiving agency complies with the security and management control outsourcing standard for non-channelers (see Exhibit A).
140. NCJA is responsible for compliance to technical standards set forth by WSP and the CJIS Security Policy.
141. NCJA will conduct periodic self audits to ensure compliance with CJIS Security Policy.
142. NCJA will participate in WSP and FBI audits, provide plans for any compliance issues, and follow through to resolution within identified timeframes.
143. NCJA will ensure all appropriate staff members are trained according to the state and federal requirements.

### **III. CRIMINAL HISTORY RECORD INFORMATION RESPONSIBILITIES**

NCJA shall conform to system policies, as established by the FBI CJIS Division and WSP, before access to CHRI is permitted. This will allow for control over the data and give assurance of system security.

31. The rules and procedures governing access to CHRI shall apply equally to all participants in the system.
32. All noncriminal justice agencies with access to CHRI data must designate a specific unit, position, or personnel to access CHRI; noncriminal justice agencies must advise WSP of such personnel and changes to such designation.
33. All noncriminal justice agencies with access to CHRI data from the system shall permit an FBI CJIS Division or WSP audit team to conduct appropriate audits. NCJA must cooperate with these audits and respond promptly.

### **IV. SECURITY RESPONSIBILITIES**

#### **Technical Roles and Responsibilities**

NCJA must comply with and enforce system security. NCJA must have someone designated as the security point of contact (POC). Security POC's shall be responsible for the following:

61. Identifying the user of the hardware/software and ensuring that no unauthorized users have access to the same.
62. Identifying and documenting how the equipment is connected to the state system.

63. Ensuring that personnel security screening procedures are being followed as stated in the CJIS Security Policy.
64. Ensuring that appropriate hardware security measures are in place.
65. Supporting policy compliance and keeping the WSP informed of security incidents.
66. If the technical POC changes at your agency, notify WSP immediately.

#### **Security Enforcement**

NCJA is responsible for enforcing system security standards for their agency, in addition to all of the other agencies to which the NCJA provides CHRI information. Authorized users shall access and disseminate the CHRI data only for the purpose for which they are authorized. NCJA shall have a written policy for the discipline of policy violators.

#### **Technical Security Training**

All Information Technology (IT) employees who have access to and those who have direct responsibility to configure and maintain FBI CJIS systems must review security awareness training within six months of their appointment or assignment. Documentation pertaining to the materials used and those employees which receive security awareness training shall be maintained in a current status.

#### **Physical Security**

A physically secured location in a noncriminal justice facility, an area, a room, a group of rooms, that is/are subject to criminal justice agency management control security addendum and which contain hardware, software, and/or firmware (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch panels, etc.) that provide access to the CJIS sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that restrict unauthorized access.

All personnel with access to computer centers, CHRI, or areas where CHRI information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check. All personnel must review security awareness training within six months of their appointment or assignment.

#### **Personnel Security**

To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days of initial employment or assignment for all personnel who have authorized access to FBI CJIS information and those who have direct responsibility to configure and maintain computer systems and networks with access to FBI CJIS information. All requests from system access shall be made as specified by the CJIS Systems Officer (i.e. WSP Identification and Criminal History Section).

- gg. NCJA shall use the data supplied by WSP and the FBI under this MOU only for the authorized purpose intended. NCJA shall not use this data for any other purpose and shall not disseminate this data with any other parties unless required by law. NCJA shall share any public disclosure requests regarding this data with the WSP.

#### **Storage**

Please see 'Security and Management Control Outsourcing Standard for Non-Channelers' (Exhibit A).



**V. LIAISON REPRESENTATIVES**

**For the Washington State Patrol:**

Jim Anderson, Administrator  
Criminal Records Division  
PO Box 42619  
Olympia WA 98504-2619  
Phone: (360) 534-2101  
Fax: (360) 534-2070  
E-mail: [jim.anderson@wsp.wa.gov](mailto:jim.anderson@wsp.wa.gov)

**For the Washington State  
Investment Board:**

Joan Samuelson  
PO Box 40916  
Olympia WA 98504  
360-956-4716  
[jsamuelson@sib.wa.gov](mailto:jsamuelson@sib.wa.gov)

**VI. INDEMNIFICATION**

Each party shall defend, protect and hold harmless the other party from and against all claims, suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing this MOU.

**VII. PERIOD OF MOU**

This MOU becomes effective on the date of the last signature and continues for three years and may be renewed. It may be modified by mutual written consent of the two agencies. Liaison Representatives may modify Exhibit A by mutual written consent of the two agencies without changing the general conditions of this MOU.

**VIII. TERMINATION**

Except as otherwise provided in this MOU, either party may terminate this MOU upon ninety (90) days' written notification to the other party. If this MOU is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this MOU for performance prior to the effective date of termination.

**IX. DISPUTES**

In the event that a dispute arises under this MOU, it shall be determined in the following manner: The Chief of WSP, or designee, shall appoint one member to the Dispute Board. NCJA shall appoint one member to the Dispute Board. The Chief of WSP, or designee, and the NCJA shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. If applicable and as an alternative to this process, either of the parties may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.

**X. EXHIBITS**

The exhibits listed below are incorporated into and made a part of this MOU:

Exhibit A - 'Security and Management Control Outsourcing Standard for Non-Channelers'

Exhibit B - 'CJIS Security Policy'

**XI. ORDER OF PRECEDENCE**

In the event of any inconsistency in the terms of this MOU, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

- oo. Applicable federal and state statutes and regulations;
- pp. The Terms and Conditions contained in this MOU;
- qq. The Exhibits attached to this MOU;
- rr. Any other provisions of the MOU, whether incorporated by reference or otherwise.

**XII. ALL WRITINGS CONTAINED HEREIN**

This MOU contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this MOU shall be deemed to exist or to bind any of the parties hereto.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

WASHINGTON STATE  
INVESTMENT BOARD

\_\_\_\_\_  
John R. Batiste, Chief

\_\_\_\_\_

\_\_\_\_\_  
Date

\_\_\_\_\_  
Date

## SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD for NON-CHANNELERS

The goal of this document is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the Contractor. Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security and Management Control Outsourcing Standard (Outsourcing Standard) is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI without a direct connection to the FBI CJIS Wide Area Network (WAN).

### 1.0 *Definitions*

- 1.01 *Access to CHRI* means to view or make use of CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by title 42, United States Code, section 14614(b).
- 1.02 *Authorized Recipient* means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.
- 1.03 *Chief Administrator* means the primary administrator of a Nonparty State’s criminal history record repository or a designee of such administrator who is

a regular full-time employee of the repository, which is also referred to as the State Identification Bureau (SIB) Chief.

- 1.04 *CHRI*, as referred to in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.
- 1.05 *Criminal History Record Check*, for purposes of this Outsourcing Standard only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.
- 1.06 *Compact Officer*, as provided in Article I(2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the compact among federal agencies], or (B) with respect to a Party State, the chief administrator of the State's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.
- 1.07 *Contractor* means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI.
- 1.08 *Dissemination* means the disclosure of CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 1.09 *Noncriminal Justice Administrative Functions* means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:
1. Making fitness determinations/recommendations
  2. Obtaining missing dispositions
  3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General
  4. Other authorized activities relating to the general handling, use, and storage of CHRI

- 1.10 *Noncriminal Justice Purposes*, as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.
- 1.11 *Outsourcing Standard* means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. This Outsourcing Standard authorizes access to CHRI for noncriminal justice purposes, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.
- 1.12 *Physically Secure Location* means a facility or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CHRI and associated information systems.
- 1.13 *Positive Identification*, as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints<sup>1</sup> or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other non-unique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.
- 1.14 *Public Carrier Network* means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: Dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.
- 1.15 *Security Violation* means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in

---

<sup>1</sup> The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning positive identification may be obtained from the FBI Compact Council office.

violation of: (A) Federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

2.0 *Responsibilities of the Authorized Recipient*

- 2.01 Prior to engaging in outsourcing any noncriminal justice administrative functions, the Authorized Recipient shall: (a) Request and receive written permission from (1) the State Compact Officer/Chief Administrator<sup>2</sup> or (2) the FBI Compact Officer<sup>3</sup>; (b) provide the Compact Officer/Chief Administrator copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested; and (c) inquire of the FBI Compact Officer whether a prospective Contractor has any security violations (See Section 8.04). The FBI Compact Officer will report those findings to the Authorized Recipient and, when applicable, to the State Compact Officer/Chief Administrator.
- 2.02 The Authorized Recipient shall execute a contract or agreement prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.
- 2.03 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; limit retention of the information to a period of time not to exceed that period of time the Authorized Recipient is permitted to retain such information; prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General; ensure the security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; and ensure that Contractor

---

<sup>2</sup>The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and Authorized Recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.

<sup>3</sup>State or local Authorized Recipients based on State or Federal Statutes shall contact the State Compact Officer/Chief Administrator. Federal or Regulatory Agency Authorized Recipients shall contact the FBI Compact Officer.

personnel comply with this Outsourcing Standard.

- a. The Authorized Recipient shall conduct criminal history record checks of Contractor personnel having access to CHRI if such checks are required or authorized of the Authorized Recipient's personnel having similar access.<sup>4</sup> The Authorized Recipient shall maintain updated records of Contractor personnel who have access to CHRI and update those records within 24 hours when changes to that access occur and, if a criminal history record check is required, the Authorized Recipient shall maintain a list of Contractor personnel who successfully completed the criminal history record check.
  - b. The Authorized Recipient shall ensure that the Contractor maintains site security.
  - c. The Authorized Recipient shall ensure that the most current version of both the Outsourcing Standard and the CJIS Security Policy are incorporated by reference at the time of contract, contract renewal, or within 30 calendar days (unless otherwise directed) of notification of successor versions of the Outsourcing Standard and/or CJIS Security Policy, whichever is sooner. The Authorized Recipient shall notify the Contractor within 30 calendar days (unless otherwise directed) of FBI notification regarding changes or updates to the Outsourcing Standard and/or CJIS Security Policy.
- 2.04 The Authorized Recipient shall understand the communications and record capabilities of the Contractor which has access to federal or state records through, or because of, its outsourcing relationship with the Authorized Recipient. The Authorized Recipient shall maintain an updated topological drawing which depicts the interconnectivity of the Contractor's network configuration.
- 2.05 The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the Outsourcing Standard. The Authorized Recipient shall certify to the Compact Officer/Chief Administrator that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.

---

<sup>4</sup>If a national criminal history record check of Authorized Recipient personnel having access to CHRI is mandated or authorized by a federal statute, executive order, or state statute approved by the Attorney General under Public Law 92-544, the State Compact Officer/Chief Administrator and/or the FBI Compact Officer must ensure Contractor personnel having similar access are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives. The national criminal history record checks of Contractor personnel with access to CHRI cannot be outsourced and must be performed by the Authorized Recipient.

2.06 The Authorized Recipient shall provide written notice of any early voluntary termination of the contract to the Compact Officer/Chief Administrator or the FBI Compact Officer.

3.0 *Responsibilities of the Contractor*

3.01 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the CJIS Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

3.02 The Contractor shall develop, document, administer, and maintain a Security Program (Physical, Personnel, and Information Technology) to comply with the most current Outsourcing Standard and the most current FBI *CJIS Security Policy*. The Security Program shall describe the implementation of the security requirements described in this Outsourcing Standard and the FBI *CJIS Security Policy*. In addition, the Contractor is also responsible to set, maintain, and enforce the standards for the selection, supervision, and separation of personnel who have access to CHRI. The Authorized Recipient shall provide the written approval of a Contractor's Security Program.

3.03 The requirements for a Security Program should include, at a minimum:

- a) Description of the implementation of the security requirements described in this Outsourcing Standard and the *CJIS Security Policy*.
- b) Security Training.
- c) Guidelines for documentation of security violations.
- d) Standards for the selection, supervision, and separation of personnel with access to CHRI.

\*\*If the Contractor is using a corporate policy, it must meet the requirements outlined in this Outsourcing Standard and the *CJIS Security Policy*. If the corporate policy is not this specific, it must flow down to a level where the documentation supports these requirements.

3.04 Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. The Authorized Recipient shall review and provide to the Contractor written approval of the Security Training Program. Training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall annually, not later than the anniversary date of the contract, certify in writing to the Authorized Recipient that annual refresher training was completed for those Contractor personnel with access



to CHRI.

- 3.05 The Contractor shall make its facilities available for announced and unannounced audits performed by the Authorized Recipient, the state, or the FBI on behalf of the Compact Council.
- 3.06 The Contractor's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI CJIS Division. During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.
- 3.07 The Contractor shall maintain CHRI only for the period of time necessary to fulfill its contractual obligations but not to exceed the period of time that the Authorized Recipient is authorized to maintain and does maintain the CHRI.
- 3.08 The Contractor shall maintain a log of any dissemination of CHRI, for a minimum of 365 days.

#### 4.0 *Site Security*

- 4.01 The Authorized Recipient shall ensure that the Contractor site(s) is a physically secure location to protect against any unauthorized access to CHRI.

#### 5.0 *Dissemination*

- 5.01 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 5.02 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) The Authorized Recipient and the secondary recipient with unique identifiers, (B) the record disseminated, (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.
- 5.03 If CHRI is stored or disseminated in an electronic format, the Contractor shall protect against unauthorized access to the equipment and any of the data. In no event shall responses containing CHRI be disseminated other than as governed by this Outsourcing Standard or more stringent contract requirements.

#### 6.0 *Personnel Security*

- 6.01 If a local, state, or federal written standard requires or authorizes a criminal history record check of the Authorized Recipient's personnel with access to

CHRI, then a criminal history record check shall be required of the Contractor's (and approved Sub-Contractor's) employees having access to CHRI. Criminal history record checks of Contractor and approved Sub-Contractor employees, at a minimum, will be no less stringent than criminal history record checks that are performed on the Authorized Recipient's personnel performing similar functions. Criminal history record checks must be completed prior to accessing CHRI under the contract.

- 6.02 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm in writing that each employee has certified in writing that he/she understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities. The Contractor shall maintain the employee certifications in a file that is subject to review during audits. Employees shall make such certification prior to performing work under the contract.
- 6.03 The Contractor shall maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur, and if a criminal history record check is required, maintain a list of personnel who have successfully completed criminal history record checks. The Contractor shall notify Authorized Recipients within 24 hours when additions or deletions occur.

## 7.0 *System Security*

- 7.01 The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy.
  - a. If CHRI can be accessed by unauthorized personnel via Wide Area Network/Local Area Network or the Internet, then the Contractor shall protect the CHRI with firewall-type devices to prevent such unauthorized access. These devices shall implement a minimum firewall profile as specified by the CJIS Security Policy in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.
  - b. Data encryption shall be required throughout the network passing CHRI through a shared public carrier network.
- 7.02 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.
  - a. CHRI shall be stored in a physically secure location.
  - b. The Authorized Recipient shall ensure that a procedure is in place for

sanitizing all fixed storage media (e.g., disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal, or reuse. Sanitization procedures include overwriting the media and/or degaussing the media.

- c. The Authorized Recipient shall ensure that a procedure is in place for the disposal or return of all non-fixed storage media (e.g., hard copies, print-outs).
- 7.03 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient, Contractor, or sub-Contractor must be assigned a unique identifying number.

## 8.0 *Security Violations*

### 8.01 Duties of the Authorized Recipient and Contractor

- a. The Contractor shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference.
- b. Pending investigation, the Contractor shall, upon detection or awareness, suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.
- c. The Contractor shall immediately (within four hours) notify the Authorized Recipient of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. Within five calendar days of such notification, the Contractor shall provide the Authorized Recipient a written report documenting such security violation, any corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.
- d. The Authorized Recipient shall immediately (within four hours) notify the State Compact Officer/Chief Administrator and the FBI Compact Officer of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator, if applicable, and the FBI Compact Officer, within five calendar days of receipt of the written report from the Contractor. The written report must include any corrective actions taken by the Contractor and the Authorized Recipient to resolve such security violation.

- 8.02 Termination of the contract by the Authorized Recipient for security violations
- a. The contract is subject to termination by the Authorized Recipient for security violations involving CHRI obtained pursuant to the contract.
  - b. The contract is subject to termination by the Authorized Recipient for the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.
  - c. If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient shall terminate the contract.
- 8.03 Suspension or termination of the exchange of CHRI for security violations
- a. Notwithstanding the actions taken by the State Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Compact Council or the United States Attorney General may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 CFR §906.2(d).
  - b. If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United States Attorney General by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be deleted or returned in accordance with the provisions and time frame as specified by the Authorized Recipient.
- 8.04 The Authorized Recipient shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following:
- a. The termination of a contract for security violations.
  - b. Security violations involving the unauthorized access to CHRI.
  - c. The Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.
- 8.05 The Compact Officer/Chief Administrator, Compact Council and the United States Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.
- 8.06 The Compact Officer/Chief Administrator, Compact Council, and the United

States Attorney General reserve the right to audit the Authorized Recipient and the Contractor's operations and procedures at scheduled or unscheduled times. The Compact Council, the United States Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the contract.

9.0 *Miscellaneous Provisions*

- 9.01 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, Compact Officer/Chief Administrator (where applicable), and the FBI.
- 9.02 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) The CJIS Security Policy.
- 9.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and the CHRI accessed therefrom and it is understood that there may be terms and conditions of the appended contract which impose more stringent requirements upon the Contractor.<sup>5</sup>
- 9.04 The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. Conformance to such security measures may not be less stringent than stated in this Outsourcing Standard without the consent of the Compact Council in consultation with the United States Attorney General.
- 9.05 This Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.
- 9.06 Appropriate notices, assurances, and correspondence to the FBI Compact Officer, Compact Council, and the United States Attorney General required by Section 8.0 of this Outsourcing Standard shall be forwarded by First Class Mail to:

FBI Compact Officer  
1000 Custer Hollow Road  
Module D-3  
Clarksburg, WV 26306

10.0 *Exemption from Above Provisions*

---

<sup>5</sup>Such conditions could include additional audits, fees, or security requirements. The Compact Council, Authorized Recipients, and the Compact Officer/Chief Administrator have the explicit authority to require more stringent standards than those contained in the Outsourcing Standard.

- 10.01 An Information Technology (IT) contract need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:
1. Access to CHRI by the IT contractor's personnel is limited solely for the development and/or maintenance of the Authorized Recipient's computer system;
  2. Access to CHRI is incidental, but necessary, to the duties being performed by the IT contractor;
  3. The computer system resides within the Authorized Recipient's facility;
  4. The Authorized Recipient's personnel supervise or work directly with the IT contractor personnel;
  5. The Authorized Recipient maintains complete, positive control of the IT contractor's access to the computer system and CHRI contained therein; and
  6. The Authorized Recipient retains all of the duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard.

- 10.02 An Authorized Recipient's contract where access to CHRI is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 4.0, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:
1. Access to CHRI by the Contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient;
  2. Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor;

3. The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the Authorized Recipient;
4. The Contractor's personnel are subject to the same criminal history record checks as the Authorized Recipient's personnel;
5. The criminal history record checks of the Contractor personnel are completed prior to work on the contract or agreement;
6. The Authorized Recipient retains all other duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard; and
7. The Contractor stores the CHRI in a physically secure location.

**WSP Contract No. C130706GSC  
Amendment 1**

**WASHINGTON STATE PATROL  
CONTRACT AMENDMENT**

The above referenced Contract between the Washington State Patrol and the Washington State Investment Board is hereby amended as follows:

- The end date shall be extended through September 19, 2021.
- EXHIBIT B CJIS Security Policy 5.1 shall be replaced with EXHIBIT B CJIS Security Policy 5.6.

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL



FOR: John R. Batiste, Chief

  
Date

WASHINGTON STATE  
INVESTMENT BOARD

  
Signature  
Date



WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above referenced Contract between the Washington State Patrol and the Washington State Gambling Commission is hereby amended as follows:

- The end date shall be extended through March 25, 2022.
- Exhibit B "CJIS Security Policy" shall be replaced by Exhibit B – Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.5, published 6/1/2016 which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL



FOR: John R. Batiste, Chief

4/3/17

Date

WASHINGTON STATE GAMBLING  
COMMISSION



Signature

3 APRIL 2017

Date

**MEMORANDUM OF UNDERSTANDING**

**Between the**

**WASHINGTON STATE PATROL**

**And the**

**WASHINGTON STATE  
GAMBLING COMMISSION**

**I. PURPOSE**

The parties to this Memorandum of Understanding (MOU) are the Washington State Patrol, Identification and Criminal History Section (WSP) and the Washington State Gambling Commission (WSGC). The WSGC is a limited law enforcement agency with powers to investigate violations of and enforce the provisions of Title 9.46 RCW including the penal laws relating to the conduct of or participation in gambling activities. RCW 9.46.070(7) requires the WSGC to conduct fingerprinting and national criminal history background checks for persons seeking licensure to participate in authorized gambling activities. The statute also states that the national criminal history background checks shall be conducted using fingerprints submitted to the United States Department of Justice-Federal Bureau of Investigation (FBI).

Pursuant to RCW 9.46.210(4), criminal justice agencies may disseminate criminal history record information (CHRI) that includes nonconviction data to the WSGC "for any purpose associated with the investigation for suitability for involvement" in authorized gambling activities. This MOU, therefore, sets forth the policy to ensure the protection of CHRI exchanged between the WSP, WSGC, and the FBI. This MOU provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CHRI data. This policy applies to the WSGC and its contractors with access to, or who operate in support of, non-criminal justice functions and information, including licensing.

**II. ADMINISTRATIVE RESPONSIBILITIES**

As participants in this MOU, the parties will develop mutually and separately appropriate procedures for transmission, dissemination, storage, and destruction of CHRI data.

- a. The Washington State Patrol. WSP shall ensure the WSGC complies with the Criminal Justice Information Services (CJIS) Security Policy (Exhibit B), which includes authorized use of CHRI, dissemination of CHRI, statute authorization for civil applicant background checks conducted by noncriminal justice agencies, applicant notification and record challenges, security of CHRI, storage of CHRI, outsourcing of noncriminal justice administrative functions, and user fees. WSP will conduct regional audits of all agencies working under this MOU to ensure compliance with all state and federal standards.
- b. Washington State Gambling Commission. The WSGC shall be responsible for ensuring:
  1. WSGC responds to requests for information by the FBI CJIS Division or the WSP in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of the agency.

2. WSGC has formalized written procedures for the following, if applicable: criminal history use and dissemination, misuse, background checks, password management, storage, and destruction of CHRI.
3. CHRI received as a result of licensing or employment purposes, pursuant to Public Law 92-544, is solely used for the purpose for which the record was requested. Subject fingerprints shall be submitted with all requests for CHRI for noncriminal justice purposes. Access to the FBI CJIS using name-based inquiry and record request messages is not permitted for noncriminal justice purposes, unless otherwise approved by the FBI.
4. Access to CHRI by authorized officials is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or other authorized entities.
5. All fingerprint based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.
6. WSGC must notify the applicants fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The officials making the determination of suitability for licensing or employment shall provide the applicants the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record. These officials also must advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in Title 28, C.F.R. 16.34. WSGC should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so.
7. Appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity.
8. WSGC shall seek WSP permission prior to outsourcing noncriminal justice functions.
9. Outsourcing of noncriminal justice administrative functions requiring access to CHRI to either another governmental agency or a private contractor acting as an agent for the authorized receiving agency complies with the security and management control outsourcing standard for non-channelers (Exhibit A).
10. WSGC is responsible for compliance to technical standards set forth by WSP and the CJIS Security Policy.
11. WSGC will conduct periodic self audits to ensure compliance with CJIS Security Policy.
12. WSGC will participate in WSP and FBI audits, provide plans for any compliance issues, and follow through to resolution within identified timeframes.
13. WSGC will ensure all appropriate staff members are trained according to the state and federal requirements.

### **III. CRIMINAL HISTORY RECORD INFORMATION RESPONSIBILITIES**

WSGC shall conform to system policies, as established by the FBI CJIS Division and WSP, before access to CHRI is permitted. This will allow for control over the data and give assurance of system security.

1. The rules and procedures governing access to CHRI shall apply equally to all participants in the system.
2. WSGC will designate the specific unit, position, or personnel having access to CHRI and will advise WSP of such personnel and any changes to such designation.
3. WSGC will permit an FBI CJIS Division or WSP audit team to conduct appropriate audits and will cooperate with these audits and respond promptly.

## **IV. SECURITY RESPONSIBILITIES**

### **a. Technical Roles and Responsibilities**

WSGC must comply with and enforce system security. WSGC must have someone designated as the security point of contact (POC). Security POC's shall be responsible for the following:

1. Identifying the user of the hardware/software and ensuring that no unauthorized users have access to the same.
2. Identifying and documenting how the equipment is connected to the state system.
3. Ensuring that personnel security screening procedures are being followed as stated in the CJIS Security Policy.
4. Ensuring that appropriate hardware security measures are in place.
5. Supporting policy compliance and keeping the WSP informed of security incidents.
6. Notifying the WSP immediately if the security POC changes at the WSGC.

### **b. Security Enforcement**

WSGC is responsible for enforcing system security standards for the agency, in addition to all of the other agencies to which the WSGC provides CHRI information. Authorized users shall access and disseminate the CHRI data only for the purpose for which they are authorized. WSGC shall have a written policy for the discipline of policy violators.

### **c. Technical Security Training**

All Information Technology (IT) employees who have access to and those who have direct responsibility to configure and maintain FBI CJIS systems must review security awareness training within six months of their appointment or assignment. Documentation pertaining to the materials used and those employees which receive security awareness training shall be maintained in a current status.

### **d. Physical Security**

A physically secured location in a facility, an area, a room, a group of rooms, that is/are subject to criminal justice agency management control security addendum and which contain hardware, software, and/or firmware (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch panels, etc.) that provide access to the CJIS sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that restrict unauthorized access.

All personnel with access to computer centers, CHRI, or areas where CHRI information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check. All personnel must review security awareness training within six months of their appointment or assignment.

### **e. Personnel Security**

To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days of initial employment or assignment for all personnel who have authorized access to FBI CJIS information and those who have direct responsibility to configure and maintain computer systems and networks with access to FBI CJIS information. All requests from system access

shall be made as specified by the CJIS Systems Officer (i.e. WSP Identification and Criminal History Section).

**f. Storage**

Please see 'Security and Management Control Outsourcing Standard for Non-Channelers (Exhibit A).

**V. USE OF RECORDS**

The WSGC shall use the data supplied by WSP and the FBI under this MOU only for the authorized purpose intended. WSGC shall not use this data for any other purpose and shall not disseminate this data with any other persons or entities unless required by law. WSGC shall share any public disclosure requests regarding this data with the WSP.

**VI. LIAISON REPRESENTATIVES**

**Washington State Patrol:**  
Jim Anderson, Administrator  
Criminal Records Division  
PO Box 42619  
Olympia WA 98504-2619  
Phone: (360) 534-2101  
Fax:(360) 534-2070  
E-mail: [jim.anderson@wsp.wa.gov](mailto:jim.anderson@wsp.wa.gov)

**Washington State Gambling Commission:**  
Dave Trujillo, Director  
PO Box 42400  
Olympia WA 98504-2400  
360-486-3571  
Email: [dave.trujillo@wsgc.wa.gov](mailto:dave.trujillo@wsgc.wa.gov)

**VII. INDEMNIFICATION**

Each party shall defend, protect and hold harmless the other party from and against all claims, suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing this MOU

**VIII. PERIOD OF MOU**

This MOU becomes effective on the date of the last signature and continues for three years and may be renewed. It may be modified by mutual written consent of the two agencies. Liaison Representatives may modify Exhibit A by mutual written consent of the two agencies without changing the general conditions of this MOU.

**IX. TERMINATION**

Except as otherwise provided in this MOU, either party may terminate this MOU upon ninety (90) days written notification to the other party. If this MOU is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this MOU for performance prior to the effective date of termination.

**X. DISPUTES**

In the event that a dispute arises under this MOU, it shall be determined by a Dispute Board in the following manner: The Chief of WSP, or designee, shall appoint one member to the Dispute Board. WSGC shall appoint one member to the Dispute Board. The Chief of WSP, or designee, and the WSGC shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make

a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. If applicable and as an alternative to this process, either of the parties may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.

**XI. EXHIBITS**

The exhibits listed below are incorporated into and made a part of this MOU:

Exhibit A - 'Security and Management Control Outsourcing Standard for Non-Channelers

Exhibit B - Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.2, published 8/9/2013 which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

**XII. ORDER OF PRECEDENCE**

In the event of any inconsistency in the terms of this MOU, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

- a. Applicable federal and state statutes and regulations;
- b. The Terms and Conditions contained in this MOU;
- c. The Exhibits attached to this MOU;
- d. Any other provisions of the MOU, whether incorporated by reference or otherwise.

**XIII. ALL WRITINGS CONTAINED HEREIN**

This MOU contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this MOU shall be deemed to exist or to bind any of the parties hereto.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

WASHINGTON STATE  
GAMBLING COMMISSION

*for*   
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_  
David Trujillo, Director

*3/26/14*  
\_\_\_\_\_  
Date

*3-24-14*  
\_\_\_\_\_  
Date

## SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD for NON-CHANNELERS

The goal of this document is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the Contractor. Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security and Management Control Outsourcing Standard (Outsourcing Standard) is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI without a direct connection to the FBI CJIS Wide Area Network (WAN).

### 1.0 Definitions

- 1.01 *Access to CHRI* means to view or make use of CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by title 42, United States Code, section 14614(b).
- 1.02 *Authorized Recipient* means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.
- 1.03 *Chief Administrator* means the primary administrator of a Nonparty State’s criminal history record repository or a designee of such administrator who is

a regular full-time employee of the repository, which is also referred to as the State Identification Bureau (SIB) Chief.

- 1.04 *CHRI*, as referred to in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.
- 1.05 *Criminal History Record Check*, for purposes of this Outsourcing Standard only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.
- 1.06 *Compact Officer*, as provided in Article I(2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the compact among federal agencies], or (B) with respect to a Party State, the chief administrator of the State's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.
- 1.07 *Contractor* means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI.
- 1.08 *Dissemination* means the disclosure of CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 1.09 *Noncriminal Justice Administrative Functions* means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:
1. Making fitness determinations/recommendations
  2. Obtaining missing dispositions
  3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General
  4. Other authorized activities relating to the general handling, use, and storage of CHRI



- 1.10 *Noncriminal Justice Purposes*, as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.
- 1.11 *Outsourcing Standard* means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. This Outsourcing Standard authorizes access to CHRI for noncriminal justice purposes, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.
- 1.12 *Physically Secure Location* means a facility or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CHRI and associated information systems.
- 1.13 *Positive Identification*, as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints<sup>1</sup> or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other non-unique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.
- 1.14 *Public Carrier Network* means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: Dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.
- 1.15 *Security Violation* means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in

---

<sup>1</sup> The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning positive identification may be obtained from the FBI Compact Council office.

violation of: (A) Federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

2.0 *Responsibilities of the Authorized Recipient*

- 2.01 Prior to engaging in outsourcing any noncriminal justice administrative functions, the Authorized Recipient shall: (a) Request and receive written permission from (1) the State Compact Officer/Chief Administrator<sup>2</sup> or (2) the FBI Compact Officer<sup>3</sup>; (b) provide the Compact Officer/Chief Administrator copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested; and (c) inquire of the FBI Compact Officer whether a prospective Contractor has any security violations (See Section 8.04). The FBI Compact Officer will report those findings to the Authorized Recipient and, when applicable, to the State Compact Officer/Chief Administrator.
- 2.02 The Authorized Recipient shall execute a contract or agreement prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.
- 2.03 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; limit retention of the information to a period of time not to exceed that period of time the Authorized Recipient is permitted to retain such information; prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General; ensure the security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; and ensure that Contractor

---

<sup>2</sup>The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and Authorized Recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.

<sup>3</sup>State or local Authorized Recipients based on State or Federal Statutes shall contact the State Compact Officer/Chief Administrator. Federal or Regulatory Agency Authorized Recipients shall contact the FBI Compact Officer.

personnel comply with this Outsourcing Standard.

- a. The Authorized Recipient shall conduct criminal history record checks of Contractor personnel having access to CHRI if such checks are required or authorized of the Authorized Recipient's personnel having similar access.<sup>4</sup> The Authorized Recipient shall maintain updated records of Contractor personnel who have access to CHRI and update those records within 24 hours when changes to that access occur and, if a criminal history record check is required, the Authorized Recipient shall maintain a list of Contractor personnel who successfully completed the criminal history record check.
  - b. The Authorized Recipient shall ensure that the Contractor maintains site security.
  - c. The Authorized Recipient shall ensure that the most current version of both the Outsourcing Standard and the CJIS Security Policy are incorporated by reference at the time of contract, contract renewal, or within 30 calendar days (unless otherwise directed) of notification of successor versions of the Outsourcing Standard and/or CJIS Security Policy, whichever is sooner. The Authorized Recipient shall notify the Contractor within 30 calendar days (unless otherwise directed) of FBI notification regarding changes or updates to the Outsourcing Standard and/or CJIS Security Policy.
- 2.04 The Authorized Recipient shall understand the communications and record capabilities of the Contractor which has access to federal or state records through, or because of, its outsourcing relationship with the Authorized Recipient. The Authorized Recipient shall maintain an updated topological drawing which depicts the interconnectivity of the Contractor's network configuration.
- 2.05 The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the Outsourcing Standard. The Authorized Recipient shall certify to the Compact Officer/Chief Administrator that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.

---

<sup>4</sup>If a national criminal history record check of Authorized Recipient personnel having access to CHRI is mandated or authorized by a federal statute, executive order, or state statute approved by the Attorney General under Public Law 92-544, the State Compact Officer/Chief Administrator and/or the FBI Compact Officer must ensure Contractor personnel having similar access are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives. The national criminal history record checks of Contractor personnel with access to CHRI cannot be outsourced and must be performed by the Authorized Recipient.

2.06 The Authorized Recipient shall provide written notice of any early voluntary termination of the contract to the Compact Officer/Chief Administrator or the FBI Compact Officer.

3.0 *Responsibilities of the Contractor*

3.01 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the CJIS Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

3.02 The Contractor shall develop, document, administer, and maintain a Security Program (Physical, Personnel, and Information Technology) to comply with the most current Outsourcing Standard and the most current FBI *CJIS Security Policy*. The Security Program shall describe the implementation of the security requirements described in this Outsourcing Standard and the FBI *CJIS Security Policy*. In addition, the Contractor is also responsible to set, maintain, and enforce the standards for the selection, supervision, and separation of personnel who have access to CHRI. The Authorized Recipient shall provide the written approval of a Contractor's Security Program.

3.03 The requirements for a Security Program should include, at a minimum:

- a) Description of the implementation of the security requirements described in this Outsourcing Standard and the *CJIS Security Policy*.
- b) Security Training.
- c) Guidelines for documentation of security violations.
- d) Standards for the selection, supervision, and separation of personnel with access to CHRI.

*\*\*If the Contractor is using a corporate policy, it must meet the requirements outlined in this Outsourcing Standard and the *CJIS Security Policy*. If the corporate policy is not this specific, it must flow down to a level where the documentation supports these requirements.*

3.04 Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. The Authorized Recipient shall review and provide to the Contractor written approval of the Security Training Program. Training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall annually, not later than the anniversary date of the contract, certify in writing to the Authorized Recipient that annual refresher training was completed for those Contractor personnel with access

- to CHRI.
- 3.05 The Contractor shall make its facilities available for announced and unannounced audits performed by the Authorized Recipient, the state, or the FBI on behalf of the Compact Council.
  - 3.06 The Contractor's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI CJIS Division. During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.
  - 3.07 The Contractor shall maintain CHRI only for the period of time necessary to fulfill its contractual obligations but not to exceed the period of time that the Authorized Recipient is authorized to maintain and does maintain the CHRI.
  - 3.08 The Contractor shall maintain a log of any dissemination of CHRI, for a minimum of 365 days.
- 4.0 *Site Security*
- 4.01 The Authorized Recipient shall ensure that the Contractor site(s) is a physically secure location to protect against any unauthorized access to CHRI.
- 5.0 *Dissemination*
- 5.01 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.
  - 5.02 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) The Authorized Recipient and the secondary recipient with unique identifiers, (B) the record disseminated, (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.
  - 5.03 If CHRI is stored or disseminated in an electronic format, the Contractor shall protect against unauthorized access to the equipment and any of the data. In no event shall responses containing CHRI be disseminated other than as governed by this Outsourcing Standard or more stringent contract requirements.
- 6.0 *Personnel Security*
- 6.01 If a local, state, or federal written standard requires or authorizes a criminal history record check of the Authorized Recipient's personnel with access to

CHRI, then a criminal history record check shall be required of the Contractor's (and approved Sub-Contractor's) employees having access to CHRI. Criminal history record checks of Contractor and approved Sub-Contractor employees, at a minimum, will be no less stringent than criminal history record checks that are performed on the Authorized Recipient's personnel performing similar functions. Criminal history record checks must be completed prior to accessing CHRI under the contract.

- 6.02 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm in writing that each employee has certified in writing that he/she understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities. The Contractor shall maintain the employee certifications in a file that is subject to review during audits. Employees shall make such certification prior to performing work under the contract.
- 6.03 The Contractor shall maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur, and if a criminal history record check is required, maintain a list of personnel who have successfully completed criminal history record checks. The Contractor shall notify Authorized Recipients within 24 hours when additions or deletions occur.

## 7.0 *System Security*

- 7.01 The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy.
  - a. If CHRI can be accessed by unauthorized personnel via Wide Area Network/Local Area Network or the Internet, then the Contractor shall protect the CHRI with firewall-type devices to prevent such unauthorized access. These devices shall implement a minimum firewall profile as specified by the CJIS Security Policy in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.
  - b. Data encryption shall be required throughout the network passing CHRI through a shared public carrier network.
- 7.02 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.
  - a. CHRI shall be stored in a physically secure location.
  - b. The Authorized Recipient shall ensure that a procedure is in place for

sanitizing all fixed storage media (e.g., disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal, or reuse. Sanitization procedures include overwriting the media and/or degaussing the media.

- c. The Authorized Recipient shall ensure that a procedure is in place for the disposal or return of all non-fixed storage media (e.g., hard copies, print-outs).
- 7.03 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient, Contractor, or sub-Contractor must be assigned a unique identifying number.

## 8.0 *Security Violations*

### 8.01 Duties of the Authorized Recipient and Contractor

- a. The Contractor shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference.
- b. Pending investigation, the Contractor shall, upon detection or awareness, suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.
- c. The Contractor shall immediately (within four hours) notify the Authorized Recipient of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. Within five calendar days of such notification, the Contractor shall provide the Authorized Recipient a written report documenting such security violation, any corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.
- d. The Authorized Recipient shall immediately (within four hours) notify the State Compact Officer/Chief Administrator and the FBI Compact Officer of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator, if applicable, and the FBI Compact Officer, within five calendar days of receipt of the written report from the Contractor. The written report must include any corrective actions taken by the Contractor and the Authorized Recipient to resolve such security violation.

- 8.02 Termination of the contract by the Authorized Recipient for security violations
- a. The contract is subject to termination by the Authorized Recipient for security violations involving CHRI obtained pursuant to the contract.
  - b. The contract is subject to termination by the Authorized Recipient for the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.
  - c. If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient shall terminate the contract.
- 8.03 Suspension or termination of the exchange of CHRI for security violations
- a. Notwithstanding the actions taken by the State Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Compact Council or the United States Attorney General may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 CFR §906.2(d).
  - b. If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United States Attorney General by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be deleted or returned in accordance with the provisions and time frame as specified by the Authorized Recipient.
- 8.04 The Authorized Recipient shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following:
- a. The termination of a contract for security violations.
  - b. Security violations involving the unauthorized access to CHRI.
  - c. The Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.
- 8.05 The Compact Officer/Chief Administrator, Compact Council and the United States Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.
- 8.06 The Compact Officer/Chief Administrator, Compact Council, and the United



States Attorney General reserve the right to audit the Authorized Recipient and the Contractor's operations and procedures at scheduled or unscheduled times. The Compact Council, the United States Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the contract.

9.0 *Miscellaneous Provisions*

- 9.01 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, Compact Officer/Chief Administrator (where applicable), and the FBI.
- 9.02 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) The CJIS Security Policy.
- 9.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and the CHRI accessed therefrom and it is understood that there may be terms and conditions of the appended contract which impose more stringent requirements upon the Contractor.<sup>5</sup>
- 9.04 The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. Conformance to such security measures may not be less stringent than stated in this Outsourcing Standard without the consent of the Compact Council in consultation with the United States Attorney General.
- 9.05 This Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.
- 9.06 Appropriate notices, assurances, and correspondence to the FBI Compact Officer, Compact Council, and the United States Attorney General required by Section 8.0 of this Outsourcing Standard shall be forwarded by First Class Mail to:

FBI Compact Officer  
1000 Custer Hollow Road  
Module D-3  
Clarksburg, WV 26306

10.0 *Exemption from Above Provisions*

---

<sup>5</sup>Such conditions could include additional audits, fees, or security requirements. The Compact Council, Authorized Recipients, and the Compact Officer/Chief Administrator have the explicit authority to require more stringent standards than those contained in the Outsourcing Standard.

- 10.01 An Information Technology (IT) contract need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:
1. Access to CHRI by the IT contractor's personnel is limited solely for the development and/or maintenance of the Authorized Recipient's computer system;
  2. Access to CHRI is incidental, but necessary, to the duties being performed by the IT contractor;
  3. The computer system resides within the Authorized Recipient's facility;
  4. The Authorized Recipient's personnel supervise or work directly with the IT contractor personnel;
  5. The Authorized Recipient maintains complete, positive control of the IT contractor's access to the computer system and CHRI contained therein; and
  6. The Authorized Recipient retains all of the duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard.

- 10.02 An Authorized Recipient's contract where access to CHRI is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 4.0, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:
1. Access to CHRI by the Contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient;
  2. Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor;

3. The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the Authorized Recipient;
4. The Contractor's personnel are subject to the same criminal history record checks as the Authorized Recipient's personnel;
5. The criminal history record checks of the Contractor personnel are completed prior to work on the contract or agreement;
6. The Authorized Recipient retains all other duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard; and
7. The Contractor stores the CHRI in a physically secure location.

**MEMORANDUM OF UNDERSTANDING**

**Between the**

**WASHINGTON STATE PATROL**

**And the**

**WASHINGTON STATE  
HORSE RACING COMMISSION**

**I. PURPOSE**

The parties to this Memorandum of Understanding (MOU) are the Washington State Patrol, Identification and Criminal History Section (WSP) and the Washington State Horse Racing Commission, a non criminal justice agency (NCJA). This MOU sets forth the policy to ensure the protection of criminal history record information (CHRI) between the WSP, the NCJA, and the Federal Bureau of Investigation (FBI). This MOU provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CHRI data. This policy applies to the NCJA and its contractors with access to, or who operate in support of, non-criminal justice services and information.

**II. ADMINISTRATIVE RESPONSIBILITIES**

As participants in this MOU, the parties will develop mutually and separately appropriate procedures for transmission, dissemination, storage, and destruction of CHRI data.

- a. The Washington State Patrol. WSP shall ensure the NCJA complies with the Criminal Justice Information Services (CJIS) Security Policy (See Exhibit B) which includes authorized use of CHRI, dissemination of CHRI, statute authorization for civil applicant background checks conducted by noncriminal justice agencies, applicant notification and record challenge, security of CHRI, storage of CHRI, outsourcing of noncriminal justice administrative functions, and user fees. WSP will conduct regional audits of all agencies working under this MOU to ensure compliance to all state and federal standards.
- b. NCJA. The NCJA shall be responsible for ensuring:
  1. NCJA responds to requests for information by the FBI CJIS Division or the WSP in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of the agency.
  2. NCJA has formalized written procedures for the following, if applicable: criminal history use and dissemination, misuse, background checks, password management, storage, and destruction of CHRI.
  3. CHRI received as a result of licensing or employment purposes, pursuant to Public Law 92-544 is solely used for the purpose for which the record was requested. Subject fingerprints shall be submitted with all requests for CHRI for noncriminal justice purposes. Access to the FBI CJIS using name-based inquiry and record request messages is not permitted for noncriminal justice purpose, unless otherwise approved by the FBI.
  4. Access to CHRI by authorized officials is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or other authorized entities.

5. All fingerprint based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.
6. NCJA must notify the applicants fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The officials making the determination of suitability for licensing or employment shall provide the applicants the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record. These officials also must advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in Title 28, C.F.R. 16.34. Official making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so.
7. Appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity.
8. NCJA shall seek WSP permission prior to outsourcing noncriminal justice functions.
9. Outsourcing of noncriminal justice administrative functions requiring access to CHRI to either another governmental agency or a private contractor acting as an agent for the authorized receiving agency complies with the security and management control outsourcing standard for non-channelers (see Exhibit A).
10. NCJA is responsible for compliance to technical standards set forth by WSP and the CJIS Security Policy.
11. NCJA will conduct periodic self audits to ensure compliance with CJIS Security Policy.
12. NCJA will participate in WSP and FBI audits, provide plans for any compliance issues, and follow through to resolution within identified timeframes.
13. NCJA will ensure all appropriate staff members are trained according to the state and federal requirements.

### **III. CRIMINAL HISTORY RECORD INFORMATION RESPONSIBILITIES**

NCJA shall conform to system policies, as established by the FBI CJIS Division and WSP, before access to CHRI is permitted. This will allow for control over the data and give assurance of system security.

1. The rules and procedures governing access to CHRI shall apply equally to all participants in the system.
2. All noncriminal justice agencies with access to CHRI data must designate a specific unit, position, or personnel to access CHRI; noncriminal justice agencies must advise WSP of such personnel and changes to such designation.
3. All noncriminal justice agencies with access to CHRI data from the system shall permit an FBI CJIS Division or WSP audit team to conduct appropriate audits. NCJA must cooperate with these audits and respond promptly.

### **IV. SECURITY RESPONSIBILITIES**

#### **Technical Roles and Responsibilities**

NCJA must comply with and enforce system security. NCJA must have someone designated as the security point of contact (POC). Security POC's shall be responsible for the following:

1. Identifying the user of the hardware/software and ensuring that no unauthorized users have access to the same.
2. Identifying and documenting how the equipment is connected to the state system.

3. Ensuring that personnel security screening procedures are being followed as stated in the CJIS Security Policy.
4. Ensuring that appropriate hardware security measures are in place.
5. Supporting policy compliance and keeping the WSP informed of security incidents.
6. If the technical POC changes at your agency, notify WSP immediately.

#### **Security Enforcement**

NCJA is responsible for enforcing system security standards for their agency, in addition to all of the other agencies to which the NCJA provides CHRI information. Authorized users shall access and disseminate the CHRI data only for the purpose for which they are authorized. NCJA shall have a written policy for the discipline of policy violators.

#### **Technical Security Training**

All Information Technology (IT) employees who have access to and those who have direct responsibility to configure and maintain FBI CJIS systems must review security awareness training within six months of their appointment or assignment. Documentation pertaining to the materials used and those employees which receive security awareness training shall be maintained in a current status.

#### **Physical Security**

A physically secured location in a noncriminal justice facility, an area, a room, a group of rooms, that is/are subject to criminal justice agency management control security addendum and which contain hardware, software, and/or firmware (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch panels, etc.) that provide access to the CJIS sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that restrict unauthorized access.

All personnel with access to computer centers, CHRI, or areas where CHRI information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check. All personnel must review security awareness training within six months of their appointment or assignment.

#### **Personnel Security**

To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days of initial employment or assignment for all personnel who have authorized access to FBI CJIS information and those who have direct responsibility to configure and maintain computer systems and networks with access to FBI CJIS information. All requests from system access shall be made as specified by the CJIS Systems Officer (i.e. WSP Identification and Criminal History Section).

- c. NCJA shall use the data supplied by WSP and the FBI under this MOU only for the authorized purpose intended. NCJA shall not use this data for any other purpose and shall not disseminate this data with any other parties unless required by law. NCJA shall share any public disclosure requests regarding this data with the WSP.

#### **Storage**

Please see 'Security and Management Control Outsourcing Standard for Non-Channelers' (Exhibit A).

**V. LIAISON REPRESENTATIVES**  
**For the Washington State Patrol:**

Jim Anderson, Administrator  
Criminal Records Division  
PO Box 42619  
Olympia WA 98504-2619  
Phone: (360) 534-2101  
Fax:(360) 534-2070  
E-mail: [jim.anderson@wsp.wa.gov](mailto:jim.anderson@wsp.wa.gov)

**For the Washington State**  
**Horse Racing Commission:**

Doug Moore  
PO Box 40906  
Olympia WA 98504  
360-459-6462  
[patty.sorby@whrc.state.wa.us](mailto:patty.sorby@whrc.state.wa.us)

**VI. INDEMNIFICATION**

Each party shall defend, protect and hold harmless the other party from and against all claims, suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing this MOU.

**VII. PERIOD OF MOU**

This MOU becomes effective on the date of the last signature and continues for three years and may be renewed. It may be modified by mutual written consent of the two agencies. Liaison Representatives may modify Exhibit A by mutual written consent of the two agencies without changing the general conditions of this MOU.

**VIII. TERMINATION**

Except as otherwise provided in this MOU, either party may terminate this MOU upon ninety (90) days' written notification to the other party. If this MOU is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this MOU for performance prior to the effective date of termination.

**IX. DISPUTES**

In the event that a dispute arises under this MOU, it shall be determined in the following manner: The Chief of WSP, or designee, shall appoint one member to the Dispute Board. NCJA shall appoint one member to the Dispute Board. The Chief of WSP, or designee, and the NCJA shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. If applicable and as an alternative to this process, either of the parties may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.

**X. EXHIBITS**

The exhibits listed below are incorporated into and made a part of this MOU:

Exhibit A - 'Security and Management Control Outsourcing Standard for Non-Channelers'

Exhibit B - Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.2, published 8/9/2013 which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

**XI. ORDER OF PRECEDENCE**

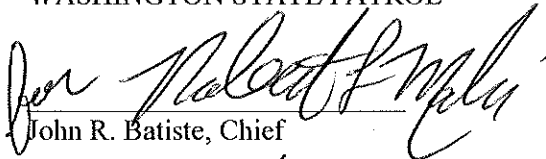
In the event of any inconsistency in the terms of this MOU, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

- a. Applicable federal and state statutes and regulations;
- b. The Terms and Conditions contained in this MOU;
- c. The Exhibits attached to this MOU;
- d. Any other provisions of the MOU, whether incorporated by reference or otherwise.

**XII. ALL WRITINGS CONTAINED HEREIN**

This MOU contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this MOU shall be deemed to exist or to bind any of the parties hereto.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

  
\_\_\_\_\_  
John R. Batiste, Chief

Date

9/16/13

WASHINGTON STATE  
HORSE RACING COMMISSION

  
\_\_\_\_\_

Date

9-11-13



## SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD for NON-CANNELERS

The goal of this document is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the Contractor. Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security and Management Control Outsourcing Standard (Outsourcing Standard) is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI without a direct connection to the FBI CJIS Wide Area Network (WAN).

### 1.0 *Definitions*

- 1.01 *Access to CHRI* means to view or make use of CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by title 42, United States Code, section 14614(b).
- 1.02 *Authorized Recipient* means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.
- 1.03 *Chief Administrator* means the primary administrator of a Nonparty State’s criminal history record repository or a designee of such administrator who is

a regular full-time employee of the repository, which is also referred to as the State Identification Bureau (SIB) Chief.

- 1.04 *CHRI*, as referred to in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.
- 1.05 *Criminal History Record Check*, for purposes of this Outsourcing Standard only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.
- 1.06 *Compact Officer*, as provided in Article I(2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the compact among federal agencies], or (B) with respect to a Party State, the chief administrator of the State's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.
- 1.07 *Contractor* means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI.
- 1.08 *Dissemination* means the disclosure of CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 1.09 *Noncriminal Justice Administrative Functions* means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:
1. Making fitness determinations/recommendations
  2. Obtaining missing dispositions
  3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General
  4. Other authorized activities relating to the general handling, use, and storage of CHRI

- 1.10 *Noncriminal Justice Purposes*, as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.
- 1.11 *Outsourcing Standard* means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. This Outsourcing Standard authorizes access to CHRI for noncriminal justice purposes, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.
- 1.12 *Physically Secure Location* means a facility or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CHRI and associated information systems.
- 1.13 *Positive Identification*, as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints<sup>1</sup> or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other non-unique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.
- 1.14 *Public Carrier Network* means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: Dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.
- 1.15 *Security Violation* means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in

---

<sup>1</sup> The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning positive identification may be obtained from the FBI Compact Council office.

violation of: (A) Federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

2.0 *Responsibilities of the Authorized Recipient*

- 2.01 Prior to engaging in outsourcing any noncriminal justice administrative functions, the Authorized Recipient shall: (a) Request and receive written permission from (1) the State Compact Officer/Chief Administrator<sup>2</sup> or (2) the FBI Compact Officer<sup>3</sup>; (b) provide the Compact Officer/Chief Administrator copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested; and (c) inquire of the FBI Compact Officer whether a prospective Contractor has any security violations (See Section 8.04). The FBI Compact Officer will report those findings to the Authorized Recipient and, when applicable, to the State Compact Officer/Chief Administrator.
- 2.02 The Authorized Recipient shall execute a contract or agreement prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.
- 2.03 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; limit retention of the information to a period of time not to exceed that period of time the Authorized Recipient is permitted to retain such information; prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General; ensure the security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; and ensure that Contractor

---

<sup>2</sup>The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and Authorized Recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.

<sup>3</sup>State or local Authorized Recipients based on State or Federal Statutes shall contact the State Compact Officer/Chief Administrator. Federal or Regulatory Agency Authorized Recipients shall contact the FBI Compact Officer.

personnel comply with this Outsourcing Standard.

- a. The Authorized Recipient shall conduct criminal history record checks of Contractor personnel having access to CHRI if such checks are required or authorized of the Authorized Recipient's personnel having similar access.<sup>4</sup> The Authorized Recipient shall maintain updated records of Contractor personnel who have access to CHRI and update those records within 24 hours when changes to that access occur and, if a criminal history record check is required, the Authorized Recipient shall maintain a list of Contractor personnel who successfully completed the criminal history record check.
  - b. The Authorized Recipient shall ensure that the Contractor maintains site security.
  - c. The Authorized Recipient shall ensure that the most current version of both the Outsourcing Standard and the CJIS Security Policy are incorporated by reference at the time of contract, contract renewal, or within 30 calendar days (unless otherwise directed) of notification of successor versions of the Outsourcing Standard and/or CJIS Security Policy, whichever is sooner. The Authorized Recipient shall notify the Contractor within 30 calendar days (unless otherwise directed) of FBI notification regarding changes or updates to the Outsourcing Standard and/or CJIS Security Policy.
- 2.04 The Authorized Recipient shall understand the communications and record capabilities of the Contractor which has access to federal or state records through, or because of, its outsourcing relationship with the Authorized Recipient. The Authorized Recipient shall maintain an updated topological drawing which depicts the interconnectivity of the Contractor's network configuration.
- 2.05 The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the Outsourcing Standard. The Authorized Recipient shall certify to the Compact Officer/Chief Administrator that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.

---

<sup>4</sup>If a national criminal history record check of Authorized Recipient personnel having access to CHRI is mandated or authorized by a federal statute, executive order, or state statute approved by the Attorney General under Public Law 92-544, the State Compact Officer/Chief Administrator and/or the FBI Compact Officer must ensure Contractor personnel having similar access are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives. The national criminal history record checks of Contractor personnel with access to CHRI cannot be outsourced and must be performed by the Authorized Recipient.

2.06 The Authorized Recipient shall provide written notice of any early voluntary termination of the contract to the Compact Officer/Chief Administrator or the FBI Compact Officer.

3.0 *Responsibilities of the Contractor*

3.01 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the CJIS Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

3.02 The Contractor shall develop, document, administer, and maintain a Security Program (Physical, Personnel, and Information Technology) to comply with the most current Outsourcing Standard and the most current FBI *CJIS Security Policy*. The Security Program shall describe the implementation of the security requirements described in this Outsourcing Standard and the FBI *CJIS Security Policy*. In addition, the Contractor is also responsible to set, maintain, and enforce the standards for the selection, supervision, and separation of personnel who have access to CHRI. The Authorized Recipient shall provide the written approval of a Contractor's Security Program.

3.03 The requirements for a Security Program should include, at a minimum:

- a) Description of the implementation of the security requirements described in this Outsourcing Standard and the *CJIS Security Policy*.
- b) Security Training.
- c) Guidelines for documentation of security violations.
- d) Standards for the selection, supervision, and separation of personnel with access to CHRI.

\*\*If the Contractor is using a corporate policy, it must meet the requirements outlined in this Outsourcing Standard and the *CJIS Security Policy*. If the corporate policy is not this specific, it must flow down to a level where the documentation supports these requirements.

3.04 Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. The Authorized Recipient shall review and provide to the Contractor written approval of the Security Training Program. Training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall annually, not later than the anniversary date of the contract, certify in writing to the Authorized Recipient that annual refresher training was completed for those Contractor personnel with access

- to CHRI.
- 3.05 The Contractor shall make its facilities available for announced and unannounced audits performed by the Authorized Recipient, the state, or the FBI on behalf of the Compact Council.
  - 3.06 The Contractor's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI CJIS Division. During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.
  - 3.07 The Contractor shall maintain CHRI only for the period of time necessary to fulfill its contractual obligations but not to exceed the period of time that the Authorized Recipient is authorized to maintain and does maintain the CHRI.
  - 3.08 The Contractor shall maintain a log of any dissemination of CHRI, for a minimum of 365 days.
- 4.0 *Site Security*
- 4.01 The Authorized Recipient shall ensure that the Contractor site(s) is a physically secure location to protect against any unauthorized access to CHRI.
- 5.0 *Dissemination*
- 5.01 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.
  - 5.02 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) The Authorized Recipient and the secondary recipient with unique identifiers, (B) the record disseminated, (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.
  - 5.03 If CHRI is stored or disseminated in an electronic format, the Contractor shall protect against unauthorized access to the equipment and any of the data. In no event shall responses containing CHRI be disseminated other than as governed by this Outsourcing Standard or more stringent contract requirements.
- 6.0 *Personnel Security*
- 6.01 If a local, state, or federal written standard requires or authorizes a criminal history record check of the Authorized Recipient's personnel with access to

CHRI, then a criminal history record check shall be required of the Contractor's (and approved Sub-Contractor's) employees having access to CHRI. Criminal history record checks of Contractor and approved Sub-Contractor employees, at a minimum, will be no less stringent than criminal history record checks that are performed on the Authorized Recipient's personnel performing similar functions. Criminal history record checks must be completed prior to accessing CHRI under the contract.

- 6.02 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm in writing that each employee has certified in writing that he/she understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities. The Contractor shall maintain the employee certifications in a file that is subject to review during audits. Employees shall make such certification prior to performing work under the contract.
- 6.03 The Contractor shall maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur, and if a criminal history record check is required, maintain a list of personnel who have successfully completed criminal history record checks. The Contractor shall notify Authorized Recipients within 24 hours when additions or deletions occur.

## 7.0 *System Security*

- 7.01 The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy.
  - a. If CHRI can be accessed by unauthorized personnel via Wide Area Network/Local Area Network or the Internet, then the Contractor shall protect the CHRI with firewall-type devices to prevent such unauthorized access. These devices shall implement a minimum firewall profile as specified by the CJIS Security Policy in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.
  - b. Data encryption shall be required throughout the network passing CHRI through a shared public carrier network.
- 7.02 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.
  - a. CHRI shall be stored in a physically secure location.
  - b. The Authorized Recipient shall ensure that a procedure is in place for



sanitizing all fixed storage media (e.g., disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal, or reuse. Sanitization procedures include overwriting the media and/or degaussing the media.

- c. The Authorized Recipient shall ensure that a procedure is in place for the disposal or return of all non-fixed storage media (e.g., hard copies, print-outs).

7.03 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient, Contractor, or sub-Contractor must be assigned a unique identifying number.

## 8.0 *Security Violations*

### 8.01 Duties of the Authorized Recipient and Contractor

- a. The Contractor shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference.
- b. Pending investigation, the Contractor shall, upon detection or awareness, suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.
- c. The Contractor shall immediately (within four hours) notify the Authorized Recipient of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. Within five calendar days of such notification, the Contractor shall provide the Authorized Recipient a written report documenting such security violation, any corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.
- d. The Authorized Recipient shall immediately (within four hours) notify the State Compact Officer/Chief Administrator and the FBI Compact Officer of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator, if applicable, and the FBI Compact Officer, within five calendar days of receipt of the written report from the Contractor. The written report must include any corrective actions taken by the Contractor and the Authorized Recipient to resolve such security violation.

- 8.02 Termination of the contract by the Authorized Recipient for security violations
- a. The contract is subject to termination by the Authorized Recipient for security violations involving CHRI obtained pursuant to the contract.
  - b. The contract is subject to termination by the Authorized Recipient for the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.
  - c. If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient shall terminate the contract.
- 8.03 Suspension or termination of the exchange of CHRI for security violations
- a. Notwithstanding the actions taken by the State Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Compact Council or the United States Attorney General may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 CFR §906.2(d).
  - b. If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United States Attorney General by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be deleted or returned in accordance with the provisions and time frame as specified by the Authorized Recipient.
- 8.04 The Authorized Recipient shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following:
- a. The termination of a contract for security violations.
  - b. Security violations involving the unauthorized access to CHRI.
  - c. The Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.
- 8.05 The Compact Officer/Chief Administrator, Compact Council and the United States Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.
- 8.06 The Compact Officer/Chief Administrator, Compact Council, and the United

States Attorney General reserve the right to audit the Authorized Recipient and the Contractor's operations and procedures at scheduled or unscheduled times. The Compact Council, the United States Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the contract.

#### 9.0 *Miscellaneous Provisions*

- 9.01 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, Compact Officer/Chief Administrator (where applicable), and the FBI.
- 9.02 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) The CJIS Security Policy.
- 9.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and the CHRI accessed therefrom and it is understood that there may be terms and conditions of the appended contract which impose more stringent requirements upon the Contractor.<sup>5</sup>
- 9.04 The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. Conformance to such security measures may not be less stringent than stated in this Outsourcing Standard without the consent of the Compact Council in consultation with the United States Attorney General.
- 9.05 This Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.
- 9.06 Appropriate notices, assurances, and correspondence to the FBI Compact Officer, Compact Council, and the United States Attorney General required by Section 8.0 of this Outsourcing Standard shall be forwarded by First Class Mail to:
  - FBI Compact Officer
  - 1000 Custer Hollow Road
  - Module D-3
  - Clarksburg, WV 26306

#### 10.0 *Exemption from Above Provisions*

---

<sup>5</sup>Such conditions could include additional audits, fees, or security requirements. The Compact Council, Authorized Recipients, and the Compact Officer/Chief Administrator have the explicit authority to require more stringent standards than those contained in the Outsourcing Standard.

- 10.01 An Information Technology (IT) contract need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:
1. Access to CHRI by the IT contractor's personnel is limited solely for the development and/or maintenance of the Authorized Recipient's computer system;
  2. Access to CHRI is incidental, but necessary, to the duties being performed by the IT contractor;
  3. The computer system resides within the Authorized Recipient's facility;
  4. The Authorized Recipient's personnel supervise or work directly with the IT contractor personnel;
  5. The Authorized Recipient maintains complete, positive control of the IT contractor's access to the computer system and CHRI contained therein; and
  6. The Authorized Recipient retains all of the duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard.

- 10.02 An Authorized Recipient's contract where access to CHRI is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 4.0, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:
1. Access to CHRI by the Contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient;
  2. Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor;

3. The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the Authorized Recipient;
4. The Contractor's personnel are subject to the same criminal history record checks as the Authorized Recipient's personnel;
5. The criminal history record checks of the Contractor personnel are completed prior to work on the contract or agreement;
6. The Authorized Recipient retains all other duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard; and
7. The Contractor stores the CHRI in a physically secure location.

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

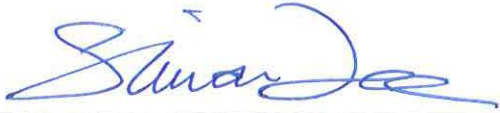
The above referenced Contract between the Washington State Patrol and Washington State Horse Racing Commission is hereby amended as follows:

- The end date shall be extended through September 15, 2021.
- EXHIBIT B CJIS Security Policy 5.1 shall be replaced with EXHIBIT B CJIS Security Policy 5.5.

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

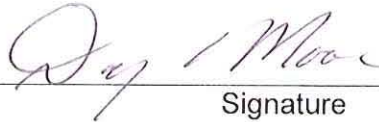


FOR: John R. Batiste, Chief

12-20-16

Date

WASHINGTON STATE HORSE  
RACING COMMISSION



Signature

12-19-16

Date

**MEMORANDUM OF UNDERSTANDING**

**Between the**

**WASHINGTON STATE PATROL**

**And the**

**EASTMONT METROPOLITAN  
PARKS DISTRICT**

**I. PURPOSE**

The parties to this Memorandum of Understanding (MOU) are the Washington State Patrol, Identification and Criminal History Section (WSP) and the Eastmont Metropolitan Parks District, a non criminal justice agency (NCJA). This MOU sets forth the policy to ensure the protection of criminal history record information (CHRI) between the WSP, the NCJA, and the Federal Bureau of Investigation (FBI). This MOU provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CHRI data. This policy applies to the NCJA and its contractors with access to, or who operate in support of, non-criminal justice services and information.

**II. ADMINISTRATIVE RESPONSIBILITIES**

As participants in this MOU, the parties will develop mutually and separately appropriate procedures for transmission, dissemination, storage, and destruction of CHRI data.

- a. The Washington State Patrol. WSP shall ensure the NCJA complies with the Criminal Justice Information Services (CJIS) Security Policy (See Exhibit B) which includes authorized use of CHRI, dissemination of CHRI, statute authorization for civil applicant background checks conducted by noncriminal justice agencies, applicant notification and record challenge, security of CHRI, storage of CHRI, outsourcing of noncriminal justice administrative functions, and user fees. WSP will conduct regional audits of all agencies working under this MOU to ensure compliance to all state and federal standards.
- b. NCJA. The NCJA shall be responsible for ensuring:
  1. NCJA responds to requests for information by the FBI CJIS Division or the WSP in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of the agency.
  2. NCJA has formalized written procedures for the following, if applicable: criminal history use and dissemination, misuse, background checks, password management, storage, and destruction of CHRI.
  3. CHRI received as a result of licensing or employment purposes, pursuant to Public Law 92-544 is solely used for the purpose for which the record was requested. Subject fingerprints shall be submitted with all requests for CHRI for noncriminal justice purposes. Access to the FBI CJIS using name-based inquiry and record request messages is not permitted for noncriminal justice purpose, unless otherwise approved by the FBI.
  4. Access to CHRI by authorized officials is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or other authorized entities.

5. All fingerprint based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.
6. NCJA must notify the applicants fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The officials making the determination of suitability for licensing or employment shall provide the applicants the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record. These officials also must advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in Title 28, C.F.R. 16.34. Official making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so.
7. Appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity.
8. NCJA shall seek WSP permission prior to outsourcing noncriminal justice functions.
9. Outsourcing of noncriminal justice administrative functions requiring access to CHRI to either another governmental agency or a private contractor acting as an agent for the authorized receiving agency complies with the security and management control outsourcing standard for non-channelers (see Exhibit A).
10. NCJA is responsible for compliance to technical standards set forth by WSP and the CJIS Security Policy.
11. NCJA will conduct periodic self audits to ensure compliance with CJIS Security Policy.
12. NCJA will participate in WSP and FBI audits, provide plans for any compliance issues, and follow through to resolution within identified timeframes.
13. NCJA will ensure all appropriate staff members are trained according to the state and federal requirements.

### **III. CRIMINAL HISTORY RECORD INFORMATION RESPONSIBILITIES**

NCJA shall conform to system policies, as established by the FBI CJIS Division and WSP, before access to CHRI is permitted. This will allow for control over the data and give assurance of system security.

1. The rules and procedures governing access to CHRI shall apply equally to all participants in the system.
2. All noncriminal justice agencies with access to CHRI data must designate a specific unit, position, or personnel to access CHRI; noncriminal justice agencies must advise WSP of such personnel and changes to such designation.
3. All noncriminal justice agencies with access to CHRI data from the system shall permit an FBI CJIS Division or WSP audit team to conduct appropriate audits. NCJA must cooperate with these audits and respond promptly.

### **IV. SECURITY RESPONSIBILITIES**

#### **Technical Roles and Responsibilities**

NCJA must comply with and enforce system security. NCJA must have someone designated as the security point of contact (POC). Security POC's shall be responsible for the following:

1. Identifying the user of the hardware/software and ensuring that no unauthorized users have access to the same.
2. Identifying and documenting how the equipment is connected to the state system.



3. Ensuring that personnel security screening procedures are being followed as stated in the CJIS Security Policy.
4. Ensuring that appropriate hardware security measures are in place.
5. Supporting policy compliance and keeping the WSP informed of security incidents.
6. If the technical POC changes at your agency, notify WSP immediately.

#### **Security Enforcement**

NCJA is responsible for enforcing system security standards for their agency, in addition to all of the other agencies to which the NCJA provides CHRI information. Authorized users shall access and disseminate the CHRI data only for the purpose for which they are authorized. NCJA shall have a written policy for the discipline of policy violators.

#### **Technical Security Training**

All Information Technology (IT) employees who have access to and those who have direct responsibility to configure and maintain FBI CJIS systems must review security awareness training within six months of their appointment or assignment. Documentation pertaining to the materials used and those employees which receive security awareness training shall be maintained in a current status.

#### **Physical Security**

A physically secured location in a noncriminal justice facility, an area, a room, a group of rooms, that is/are subject to criminal justice agency management control security addendum and which contain hardware, software, and/or firmware (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch panels, etc.) that provide access to the CJIS sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that restrict unauthorized access.

All personnel with access to computer centers, CHRI, or areas where CHRI information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check. All personnel must review security awareness training within six months of their appointment or assignment.

#### **Personnel Security**

To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days of initial employment or assignment for all personnel who have authorized access to FBI CJIS information and those who have direct responsibility to configure and maintain computer systems and networks with access to FBI CJIS information. All requests from system access shall be made as specified by the CJIS Systems Officer (i.e. WSP Identification and Criminal History Section).

- c. NCJA shall use the data supplied by WSP and the FBI under this MOU only for the authorized purpose intended. NCJA shall not use this data for any other purpose and shall not disseminate this data with any other parties unless required by law. NCJA shall share any public disclosure requests regarding this data with the WSP.

#### **Storage**

Please see 'Security and Management Control Outsourcing Standard for Non-Channelers' (Exhibit A).

**V. LIAISON REPRESENTATIVES  
For the Washington State Patrol:**

Jim Anderson, Administrator  
Criminal Records Division  
PO Box 42619  
Olympia WA 98504-2619  
Phone: (360) 534-2101  
Fax: (360) 534-2070  
E-mail: [jim.anderson@wsp.wa.gov](mailto:jim.anderson@wsp.wa.gov)

**For the Eastmont Metropolitan  
Parks District:**

Sally Brawley  
255 N Georgia Ave  
Wenatchee WA 98802  
509-884-8015  
[sbrawley@eastmontparks.com](mailto:sbrawley@eastmontparks.com)

**VI. INDEMNIFICATION**

Each party shall defend, protect and hold harmless the other party from and against all claims, suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing this MOU.

**VII. PERIOD OF MOU**

This MOU becomes effective on the date of the last signature and continues for three years and may be renewed. It may be modified by mutual written consent of the two agencies. Liaison Representatives may modify Exhibit A by mutual written consent of the two agencies without changing the general conditions of this MOU.

**VIII. TERMINATION**

Except as otherwise provided in this MOU, either party may terminate this MOU upon ninety (90) days' written notification to the other party. If this MOU is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this MOU for performance prior to the effective date of termination.

**IX. DISPUTES**

In the event that a dispute arises under this MOU, it shall be determined in the following manner: The Chief of WSP, or designee, shall appoint one member to the Dispute Board. NCJA shall appoint one member to the Dispute Board. The Chief of WSP, or designee, and the NCJA shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. If applicable and as an alternative to this process, either of the parties may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.

**X. EXHIBITS**

The exhibits listed below are incorporated into and made a part of this MOU:

Exhibit A - 'Security and Management Control Outsourcing Standard for Non-Channelers'

Exhibit B - Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.2, published 8/9/2013 which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

**XI. ORDER OF PRECEDENCE**

In the event of any inconsistency in the terms of this MOU, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

- a. Applicable federal and state statutes and regulations;
- b. The Terms and Conditions contained in this MOU;
- c. The Exhibits attached to this MOU;
- d. Any other provisions of the MOU, whether incorporated by reference or otherwise.

**XII. ALL WRITINGS CONTAINED HEREIN**

This MOU contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this MOU shall be deemed to exist or to bind any of the parties hereto.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

EASTMONT METROPOLITAN  
PARKS DISTRICT

*JR*  
  
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_

\_\_\_\_\_  
Date *9/26/13*

\_\_\_\_\_  
Date *9-18-2013*

RECEIVED  
SEP 26 2013  
EASTMONT METROPOLITAN  
PARKS DISTRICT

**MEMORANDUM OF UNDERSTANDING**

**Between the**

**WASHINGTON STATE PATROL**

**And the**

**KING COUNTY DEPENDENCY CASA**

**I. PURPOSE**

The parties to this Memorandum of Understanding (MOU) are the Washington State Patrol, Identification and Criminal History Section (WSP) and the King County Dependency CASA, a non criminal justice agency (NCJA). This MOU sets forth the policy to ensure the protection of criminal history record information (CHRI) between the WSP, the NCJA, and the Federal Bureau of Investigation (FBI). This MOU provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CHRI data. This policy applies to the NCJA and its contractors with access to, or who operate in support of, non-criminal justice services and information.

**II. ADMINISTRATIVE RESPONSIBILITIES**

As participants in this MOU, the parties will develop mutually and separately appropriate procedures for transmission, dissemination, storage, and destruction of CHRI data.

- a. The Washington State Patrol. WSP shall ensure the NCJA complies with the Criminal Justice Information Services (CJIS) Security Policy (See Exhibit B) which includes authorized use of CHRI, dissemination of CHRI, statute authorization for civil applicant background checks conducted by noncriminal justice agencies, applicant notification and record challenge, security of CHRI, storage of CHRI, outsourcing of noncriminal justice administrative functions, and user fees. WSP will conduct regional audits of all agencies working under this MOU to ensure compliance to all state and federal standards.
- b. NCJA. The NCJA shall be responsible for ensuring:
  1. NCJA responds to requests for information by the FBI CJIS Division or the WSP in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of the agency.
  2. NCJA has formalized written procedures for the following, if applicable: criminal history use and dissemination, misuse, background checks, password management, storage, and destruction of CHRI.
  3. CHRI received as a result of licensing or employment purposes, pursuant to Public Law 92-544 is solely used for the purpose for which the record was requested. Subject fingerprints shall be submitted with all requests for CHRI for noncriminal justice purposes. Access to the FBI CJIS using name-based inquiry and record request messages is not permitted for noncriminal justice purpose, unless otherwise approved by the FBI.

4. Access to CHRI by authorized officials is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or other authorized entities.
5. All fingerprint based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.
6. NCJA must notify the applicants fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The officials making the determination of suitability for licensing or employment shall provide the applicants the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record. These officials also must advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in Title 28, C.F.R. 16.34. Official making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so.
7. Appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity.
8. NCJA shall seek WSP permission prior to outsourcing noncriminal justice functions.
9. Outsourcing of noncriminal justice administrative functions requiring access to CHRI to either another governmental agency or a private contractor acting as an agent for the authorized receiving agency complies with the security and management control outsourcing standard for non-channelers (see Exhibit A).
10. NCJA is responsible for compliance to technical standards set forth by WSP and the CJIS Security Policy.
11. NCJA will conduct periodic self audits to ensure compliance with CJIS Security Policy.
12. NCJA will participate in WSP and FBI audits, provide plans for any compliance issues, and follow through to resolution within identified timeframes.
13. NCJA will ensure all appropriate staff members are trained according to the state and federal requirements.

### **III. CRIMINAL HISTORY RECORD INFORMATION RESPONSIBILITIES**

NCJA shall conform to system policies, as established by the FBI CJIS Division and WSP, before access to CHRI is permitted. This will allow for control over the data and give assurance of system security.

1. The rules and procedures governing access to CHRI shall apply equally to all participants in the system.
2. All noncriminal justice agencies with access to CHRI data must designate a specific unit, position, or personnel to access CHRI; noncriminal justice agencies must advise WSP of such personnel and changes to such designation.
3. All noncriminal justice agencies with access to CHRI data from the system shall permit an FBI CJIS Division or WSP audit team to conduct appropriate audits. NCJA must cooperate with these audits and respond promptly.

### **IV. SECURITY RESPONSIBILITIES**

#### **Technical Roles and Responsibilities**

NCJA must comply with and enforce system security. NCJA must have someone designated as the security point of contact (POC). Security POC's shall be responsible for the following:

1. Identifying the user of the hardware/software and ensuring that no unauthorized users have access to the same.
2. Identifying and documenting how the equipment is connected to the state system.
3. Ensuring that personnel security screening procedures are being followed as stated in the CJIS Security Policy.
4. Ensuring that appropriate hardware security measures are in place.
5. Supporting policy compliance and keeping the WSP informed of security incidents.
6. If the technical POC changes at your agency, notify WSP immediately.

### **Security Enforcement**

NCJA is responsible for enforcing system security standards for their agency, in addition to all of the other agencies to which the NCJA provides CHRI information. Authorized users shall access and disseminate the CHRI data only for the purpose for which they are authorized. NCJA shall have a written policy for the discipline of policy violators.

### **Technical Security Training**

All Information Technology (IT) employees who have access to and those who have direct responsibility to configure and maintain FBI CJIS systems must review security awareness training within six months of their appointment or assignment. Documentation pertaining to the materials used and those employees which receive security awareness training shall be maintained in a current status.

### **Physical Security**

A physically secured location in a noncriminal justice facility, an area, a room, a group of rooms, that is/are subject to criminal justice agency management control security addendum and which contain hardware, software, and/or firmware (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch panels, etc.) that provide access to the CJIS sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that restrict unauthorized access.

All personnel with access to computer centers, CHRI, or areas where CHRI information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check. All personnel must review security awareness training within six months of their appointment or assignment.

### **Personnel Security**

To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days of initial employment or assignment for all personnel who have authorized access to FBI CJIS information and those who have direct responsibility to configure and maintain computer systems and networks with access to FBI CJIS information. All requests from system access shall be made as specified by the CJIS Systems Officer (i.e. WSP Identification and Criminal History Section).

- c. NCJA shall use the data supplied by WSP and the FBI under this MOU only for the authorized purpose intended. NCJA shall not use this data for any other purpose and shall not disseminate this data with any other parties unless required by law. NCJA shall share any public disclosure requests regarding this data with the WSP.

**Storage**

Please see 'Security and Management Control Outsourcing Standard for Non-Channelers' (Exhibit A).

**V. LIAISON REPRESENTATIVES**

**For the Washington State Patrol:**

Jim Anderson, Administrator  
Criminal Records Division  
PO Box 42619  
Olympia WA 98504-2619  
Phone: (360) 534-2101  
Fax: (360) 534-2070  
E-mail: [jim.anderson@wsp.wa.gov](mailto:jim.anderson@wsp.wa.gov)

**For the King County Dependency CASA:**

Lisa Peterson  
1401 E Jefferson Ste 500  
Seattle WA 98122  
206-205-9705 296-1126  
[Casa.group@kingcounty.gov](mailto:Casa.group@kingcounty.gov)  
[lisa.petersen@kingcounty.gov](mailto:lisa.petersen@kingcounty.gov)

**VI. INDEMNIFICATION**

Each party shall defend, protect and hold harmless the other party from and against all claims, suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing this MOU.

**VII. PERIOD OF MOU**

This MOU becomes effective on the date of the last signature and continues for three years and may be renewed. It may be modified by mutual written consent of the two agencies. Liaison Representatives may modify Exhibit A by mutual written consent of the two agencies without changing the general conditions of this MOU.

**VIII. TERMINATION**

Except as otherwise provided in this MOU, either party may terminate this MOU upon ninety (90) days' written notification to the other party. If this MOU is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this MOU for performance prior to the effective date of termination.

**IX. DISPUTES**

In the event that a dispute arises under this MOU, it shall be determined in the following manner: The Chief of WSP, or designee, shall appoint one member to the Dispute Board. NCJA shall appoint one member to the Dispute Board. The Chief of WSP, or designee, and the NCJA shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. If applicable and as an alternative to this process, either of the parties may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.

**X. EXHIBITS**

The exhibits listed below are incorporated into and made a part of this MOU:

Exhibit A - 'Security and Management Control Outsourcing Standard for Non-Channelers'

Exhibit B - Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.2, published 8/9/2013 which is available at the following link:

[www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

**XI. ORDER OF PRECEDENCE**

In the event of any inconsistency in the terms of this MOU, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

- a. Applicable federal and state statutes and regulations;
- b. The Terms and Conditions contained in this MOU;
- c. The Exhibits attached to this MOU;
- d. Any other provisions of the MOU, whether incorporated by reference or otherwise.

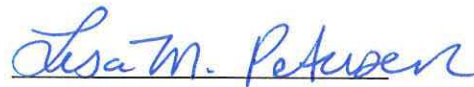
**XII. ALL WRITINGS CONTAINED HEREIN**

This MOU contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this MOU shall be deemed to exist or to bind any of the parties hereto.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

KING COUNTY DEPENDENCY CASA

  
for John R. Batiste, Chief

  
Lisa M. Peterson

3-28-14  
Date

3/25/14  
Date



## SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD for NON-CHANNELERS

The goal of this document is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the Contractor. Adequate security is defined in Office of Management and Budget Circular A-130 as security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

The intent of this Security and Management Control Outsourcing Standard (Outsourcing Standard) is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI without a direct connection to the FBI CJIS Wide Area Network (WAN).

### 1.0 Definitions

- 1.01 *Access to CHRI* means to use, exchange, retain/store, or view CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by title 42, United States Code, section 14614(b).
- 1.02 *Authorized Recipient* means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.
- 1.03 *Chief Administrator* means the primary administrator of a Nonparty State's criminal history record repository or a designee of such administrator who is a regular full-time employee of the repository.
- 1.04 *CHRI*, as referred to in Article I (4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising there from, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.

- 1.05 *Criminal History Record Check*, for purposes of this Outsourcing Standard only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.
- 1.06 *Compact Officer*, as provided in Article I (2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the compact among federal agencies], or (B) with respect to a Party State, the chief administrator of the State's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.
- 1.07 *Contractor* means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI.
- 1.08 *Dissemination* means the disclosure of CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 1.09 *Noncriminal Justice Administrative Functions* means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:
1. Making fitness determinations/recommendations
  2. Obtaining missing dispositions
  3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General
  4. Other authorized activities relating to the general handling, use, and storage of CHRI
- 1.10 *Noncriminal Justice Purposes*, as provided in Article I (18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.
- 1.11 *Outsourcing Standard* means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. The Outsourcing Standard authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.

- 1.12 *Physically Secure Location* means a location where access to CHRI can be obtained, and adequate protection is provided to prevent any unauthorized access to CHRI.
- 1.13 *Positive Identification*, as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints<sup>1</sup> or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other non-unique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.
- 1.14 *Public Carrier Network* means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: Dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.
- 1.15 *Security Violation* means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in violation of: (A) Federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

## **2.0 Responsibilities of the Authorized Recipient**

- 2.01 Prior to engaging in outsourcing any noncriminal justice administrative functions, the authorized Recipient shall: (a) Request and receive written permission from (1) the State Compact Officer/Chief Administrator<sup>2</sup> or (2) the FBI Compact Officer<sup>3</sup>; (b) provide the Compact Officer/Chief Administrator copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested; and (c) inquire of the FBI Compact Officer whether a prospective Contractor has any security violations (See Section 8.04). The FBI Compact Officer will report those findings to the Authorized Recipient and, when applicable, to the State Compact Officer/Chief Administrator.
- 2.02 The Authorized Recipient shall execute a contract or agreement prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.

---

<sup>1</sup> The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning positive identification may be obtained from the FBI Compact Council office.

<sup>2</sup> The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and Authorized Recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the terms of the contract. A representative sample will be based on generally accepted statistical sampling methods.

<sup>3</sup> State or local Authorized Recipients based on State or Federal Statutes shall contact the State Compact Officer/Chief Administrator. Federal or Regulatory Agency Authorized Recipients shall contact the FBI Compact Officer.

- 2.03 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; limit retention of the information to a period of time not to exceed that period of time the Authorized Recipient is permitted to retain such information; prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General; ensure the security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; and ensure that Contractor personnel comply with this Outsourcing Standard.
- a. The Authorized Recipient shall conduct criminal history record checks of Contractor personnel having access to CHRI if such checks are required or authorized of the Authorized Recipient's personnel having similar access.<sup>4</sup> The Authorized Recipient shall maintain updated records of Contractor personnel who have access to CHRI and update those records within 24 hours when changes to that access occur and, if a criminal history record check is required, the Authorized Recipient shall maintain a list of Contractor personnel who successfully completed the criminal history record check.
  - b. The Authorized Recipient shall ensure that the Contractor maintains site security.
  - c. The Authorized Recipient shall ensure that the most current version of both the Outsourcing Standard and the CJIS Security Policy are incorporated by reference at the time of contract, contract renewal, or within 30 calendar days (unless otherwise directed) of notification of successor versions of the Outsourcing Standard and/or CJIS Security Policy, whichever is sooner. The Authorized Recipient shall notify the Contractor within 30 calendar days (unless otherwise directed) of FBI notification regarding changes or updates to the Outsourcing Standard and/or CJIS Security Policy.
- 2.04 The Authorized Recipient shall understand the communications and record capabilities of the Contractor which has access to federal or state records through, or because of, its outsourcing relationship with the Authorized Recipient. The Authorized Recipient shall maintain an updated topological drawing which depicts the interconnectivity of the Contractor's network configuration.
- 2.05 The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the outsourcing Standard. The authorized Recipient shall certify to the Compact Officer/Chief

---

<sup>4</sup> If a national criminal history record check of government personnel having access to CHRI is mandated or authorized by a state statute approved by the Attorney General under Public Law 92-544, the State Compact Officer/Chief Administrator must ensure Contractor personnel having similar access are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives. The national criminal history record checks of Contractor personnel with access to CHRI cannot be outsourced and must be performed by the Authorized Recipient.

Administrator that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the terms of the contract.

- 2.06 The Authorized Recipient shall provide written notice of any early voluntary termination of the contract to the Compact Officer/Chief Administrator or the FBI Compact Officer.

### **3.0 Responsibilities of the Contractor**

- 3.01 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the CJIS Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 3.02 The Contractor shall develop and document a Security Program to comply with the current Outsourcing Standard and any revised or successor Outsourcing Standard. The Security Program shall describe the implementation of the security requirements described in this Outsourcing Standard, the associated Security Training Program, and the reporting guidelines for documenting and communicating security violations and corrective actions to the Authorized Recipient. The Security Program shall be subject to the written approval of the Authorized Recipient.
- 3.03 The Contractor shall be accountable for the management of the Security Program. The contractor shall be responsible for reporting all security violations of this Outsourcing Standard to the Authorized Recipient.
- 3.04 Except when the training requirement is retained by the Authorized Recipient, the contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. The Authorized Recipient shall review and provide to the contractor written approval of the Security Training Program. Training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall annually, not later than the anniversary date of the contract; certify in writing to the Authorized Recipient that annual refresher training was completed for those Contractor personnel with access to CHRI.
- 3.05 The Contractor shall make its facilities available for announced and unannounced audits performed by the Authorized Recipient, the state, or the FBI on behalf of the Compact Council.
- 3.06 The Contractor's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI CJIS Division. During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.
- 3.07 The Contractor shall maintain CHRI only for the period of time necessary to fulfill its contractual obligations but not to exceed the period of time that the Authorized Recipient is authorized to maintain and does maintain the CHRI.
- 3.08 The Contractor shall maintain a log of any dissemination of CHRI.

#### **4.0 Site Security**

- 4.01 The Authorized Recipient shall ensure that the Contractor site(s) is a physically secure location to protect against any unauthorized access to CHRI.

#### **5.0 Dissemination**

- 5.01 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 5.02 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) The Authorized Recipient and the secondary recipient with unique identifiers, (B) the record disseminated, (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.

#### **6.0 Personnel Security**

- 6.01 If a local, state, or federal written standard requires or authorizes a criminal history record check of the Authorized Recipient's personnel with access to CHRI, then a criminal history record check shall be required of the Contractor's employees having access to CHRI. The criminal history record check of Contractor employees at a minimum will be no less stringent than the criminal history record check that is performed on the Authorized Recipient's personnel performing similar functions. Criminal history record checks must be completed prior to performing work under the contract.
- 6.02 If a local, state, or federal written standard requires a criminal history record check for non-Contractor personnel who work in a physically secure location, then a criminal history record check shall be required for these individuals, unless these individuals are escorted by authorized personnel at all times. The criminal history record check for these individuals at a minimum will be no less stringent than the criminal history record check that is performed on the Authorized Recipient's non-Contractor personnel performing similar functions. Criminal history record checks must be completed prior to performing work under the contract.
- 6.03 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm in writing that each employee has certified in writing that he/she understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities. The Contractor shall maintain the employee certifications in a file that is subject to review during audits. Employees shall make such certification prior to performing work under the contract.
- 6.04 The Contractor shall maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur, and if a criminal history record check is required, maintain a list of personnel who have successfully completed criminal history record checks. The Contractor shall notify Authorized Recipients within 24 hours when additions or deletions occur.

## 7.0 System Security

- 7.01 The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy.
- a. If CHRI can be accessed by unauthorized personnel via Wide Area Network/Local Area Network or the Internet, then the Contractor shall protect the CHRI with firewall-type devices to prevent such unauthorized access. These devices shall implement a minimum firewall profile as specified by the CJIS Security Policy in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.
  - b. Data encryption shall be required throughout the network passing CHRI through a shared public carrier network.
- 7.02 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.
- a. CHRI shall be stored in a physically secure location.
  - b. The Authorized Recipient shall ensure that a procedure is in place for sanitizing all fixed storage media (e.g., disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal, or reuse. Sanitization procedures include overwriting the media and/or degaussing the media.
  - c. The Authorized Recipient shall ensure that a procedure is in place for the disposal or return of all non-fixed storage media (e.g., hard copies, print-outs).
- 7.03 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient, Contractor, or sub-Contractor must be assigned a unique identifying number.

## 8.0 Security Violations

- 8.01 Duties of the Authorized Recipient and Contractor
- a. The Contractor shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference.
  - b. Pending investigation, the Contractor shall, upon detection or awareness, suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.
  - c. The Contractor shall immediately (within four hours) notify the Authorized Recipient of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. Within five calendar days of such notification, the Contractor shall provide the Authorized Recipient a written report documenting such security violation, any corrective

actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.

- d. The Authorized Recipient shall immediately (within four hours) notify the State Compact Officer/Chief Administrator and the FBI Compact Officer of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator, if applicable, and the FBI Compact Officer, within five calendar days of receipt of the written report from the Contractor. The written report must include any corrective actions taken by the Contractor and the Authorized Recipient to resolve such security violation.

#### 8.02 Termination of the contract by the Authorized Recipient for security violations

- a. The contract is subject to termination by the Authorized Recipient for security violations involving CHRI obtained pursuant to the contract.
- b. The contract is subject to termination by the Authorized Recipient for the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.
- c. If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient shall terminate the contract.

#### 8.03 Suspension or termination of the exchange of CHRI for security violations

- a. Notwithstanding the actions taken by the State Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Compact Council or the United States Attorney General may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 C.F.R. '906.2(d).
- b. If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United States Attorney General by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be deleted or returned in accordance with the provisions and time frame as specified by the Authorized Recipient.

#### 8.04 The Authorized Recipient shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following:

- a. The termination of a contract for security violations.
- b. Security violations involving the unauthorized access to CHRI.



- c. The Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.
- 8.05 The Compact Officer/Chief Administrator, Compact Council and the United States Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.
- 8.06 The Compact Officer/Chief Administrator, Compact Council, and the United States Attorney General reserve the right to audit the Authorized Recipient and the Contractor's operations and procedures at scheduled or unscheduled times. The Compact Council, the United States Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the contract.

## 9.0 Miscellaneous Provisions

- 9.01 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, Compact Officer/Chief Administrator (where applicable), and the FBI.
- 9.02 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) The CJIS Security Policy.
- 9.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and the CHRI accessed there from and it is understood that there may be terms and conditions of the appended contract which impose more stringent requirements upon the Contractor.<sup>5</sup>
- 9.04 The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. Conformance to such security measures may not be less stringent than stated in this Outsourcing Standard without the consent of the Compact Council in consultation with the United States Attorney General.
- 9.05 This Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.
- 9.06 Appropriate notices, assurances, and correspondence to the FBI Compact Officer, Compact Council, and the United States Attorney General required by Section 8.0 of this Outsourcing Standard shall be forwarded by First Class Mail to:

FBI Compact Officer  
1000 Custer Hollow Road  
Module D-3  
Clarksburg, WV 26306

## 10.0 Exemption from Above Provisions

---

<sup>5</sup> Such conditions could include additional audits, fees, or security requirements. The Compact Council, Authorized Recipients, and the Compact Officer/Chief Administrator have the explicit authority to require more stringent standards than those contained in the Outsourcing Standard.

10.01 An Authorized Recipient that contracts with an Information Technology (IT) contractor is exempt from Sections 1.0 through 9.0 of this Outsourcing Standard when:

1. Access to CHRI by the IT contractor's personnel is limited solely for the development and/or maintenance of the authorized Recipient's computer system;
  2. Access to CHRI is incidental, but necessary, to the duties being performed by the IT contractor;
  3. The computer system resides within the Authorized Recipient's facility;
  4. The Authorized Recipient's personnel supervise or work directly with the IT contractor personnel;
  5. The Authorized Recipient maintains complete, positive control of the IT contractor's access to the computer system and CHRI contained therein;
  6. The Authorized Recipient retains all of the duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard.
- b. To utilize this exemption, the Authorized Recipient shall, at a minimum and prior to engaging in work under the contract that will allow IT contractor personnel limited access to CHRI, comply with the following requirements as an alternate method of providing adequate security, integrity, and confidentiality of CHRI:
1. Obtain written permission from the appropriate Compact Officer/Chief Administrator;
  2. Take positive actions to ensure that the IT contractor cannot access any CHRI other than that necessary to accomplish the contracted work;
  3. Execute a contract with the IT contractor which specifies the computer development and/or computer maintenance work to be performed that will result in the IT contractor's personnel having limited access to CHRI. If the IT contractor is a government agency, a Management Control Agreement is acceptable;
  4. Incorporate the CJIS Security Policy, by reference, in the contract;
  5. Maintain updated records of IT contractor personnel who have limited access to CHRI and update those records within 24 hours when changes to that access occur;

6. Perform an appropriate background investigation of each of the IT contractor's personnel with limited access to CHRI; and
7. Require each of the IT contractor's personnel with limited access to CHRI to sign a Nondisclosure Statement providing that CHRI may be disclosed only to the Authorized Recipient's personnel or other IT contractor personnel who need such information to develop or maintain the computer system, and that the CHRI shall not be further disclosed.

10.02 An Authorized Recipient that contracts with a governmental archives facility (Government Contractor) is exempt from Sections 1.0 through 9.0 of this Outsourcing Standard when:

1. Access to CHRI by the Government Contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Government Contractor's facility; (B) retrieval of the CHRI by Government Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Government Contractor personnel when not observed by the Authorized Recipient;
  2. Access to CHRI is incidental, but necessary, to the duties being performed by the Government Contractor;
  3. The Government Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the Authorized Recipient;
  4. The Government Contractor's personnel are subject to the same criminal history record checks as the Authorized Recipient's personnel;
  5. The criminal history record checks of the Government Contractor personnel are completed prior to work on the contract or agreement;
  6. The Authorized Recipient retains all other duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard; and
  7. The Government Contractor stores the CHRI in a physically secure location.
- b. To utilize this exemption, the Authorized Recipient shall, at a minimum and prior to providing CHRI to the Government Contractor, comply with the following requirements as an alternate method of providing adequate security, integrity, and confidentiality of CHRI:
1. Obtain written permission from the appropriate Compact Officer/Chief Administrator;
  2. Take positive actions to ensure that the Government Contractor cannot access any CHRI other than that necessary to accomplish the contracted work;

3. Execute a contract with the Government Contractor which specifies the work to be performed to include any storage (archiving), method of retrieval, and/or method of destruction which results in the Government Contractor's personnel having limited access to CHRI. A Management Control Agreement is also acceptable;
4. Incorporate the CJIS Security Policy, by reference, in the contract;
5. Ensure the Government Contractor's facility where the CHRI is stored is a physically secured location;
6. Maintain updated records of Government Contractor's personnel who have limited access to CHRI or access to the physically secure location where the CHRI is being stored and update those records within 24 hours when changes to that access occur;
7. Perform an appropriate criminal history record check of each of the Government Contractor's personnel, prior to their work on the contract, with limited access to CHRI or access to the physically secure location where CHRI is stored; and
8. Require each of the Government contractor's personnel with limited access to CHRI or access to the physically secure location where the CHRI is stored to sign a Nondisclosure Statement providing that CHRI may be disclosed only to the Authorized Recipient's personnel and that the CHRI shall not be further disclosed.

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above referenced Contract between the Washington State Patrol and the King County Dependency CASA is hereby amended as follows:

- The end date shall be extended through March 27, 2022.
- Exhibit B "CJIS Security Policy" shall be replaced by Exhibit B – Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.5, published 6/1/2016 which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

KING COUNTY DEPENDENCY CASA



FOR: John R. Batiste, Chief



Signature

3/23/17  
Date

3/20/17  
Date

**MEMORANDUM OF UNDERSTANDING**

**Between the**

**WASHINGTON STATE PATROL**

**And the**

**KITSAP COUNTY JUVENILE COURT**

**I. PURPOSE**

The parties to this Memorandum of Understanding (MOU) are the Washington State Patrol, Identification and Criminal History Section (WSP) and the Kitsap County Juvenile Court, a non criminal justice agency (NCJA). This MOU sets forth the policy to ensure the protection of criminal history record information (CHRI) between the WSP, the NCJA, and the Federal Bureau of Investigation (FBI). This MOU provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CHRI data. This policy applies to the NCJA and its contractors with access to, or who operate in support of, non-criminal justice services and information.

**II. ADMINISTRATIVE RESPONSIBILITIES**

As participants in this MOU, the parties will develop mutually and separately appropriate procedures for transmission, dissemination, storage, and destruction of CHRI data.

a. The Washington State Patrol. WSP shall ensure the NCJA complies with the Criminal Justice Information Services (CJIS) Security Policy (See Exhibit B) which includes authorized use of CHRI, dissemination of CHRI, statute authorization for civil applicant background checks conducted by noncriminal justice agencies, applicant notification and record challenge, security of CHRI, storage of CHRI, outsourcing of noncriminal justice administrative functions, and user fees. WSP will conduct regional audits of all agencies working under this MOU to ensure compliance to all state and federal standards.

b. NCJA. The NCJA shall be responsible for ensuring:

1. NCJA responds to requests for information by the FBI CJIS Division or the WSP in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of the agency.
2. NCJA has formalized written procedures for the following, if applicable: criminal history use and dissemination, misuse, background checks, password management, storage, and destruction of CHRI.
3. CHRI received as a result of licensing or employment purposes, pursuant to Public Law 92-544 is solely used for the purpose for which the record was requested. Subject fingerprints shall be submitted with all requests for CHRI for noncriminal justice purposes. Access to the FBI CJIS using name-based inquiry and record request messages is not permitted for noncriminal justice purpose, unless otherwise approved by the FBI.
4. Access to CHRI by authorized officials is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or other authorized entities.

5. All fingerprint based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.
6. NCJA must notify the applicants fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The officials making the determination of suitability for licensing or employment shall provide the applicants the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record. These officials also must advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in Title 28, C.F.R. 16.34. Official making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so.
7. Appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity.
8. NCJA shall seek WSP permission prior to outsourcing noncriminal justice functions.
9. Outsourcing of noncriminal justice administrative functions requiring access to CHRI to either another governmental agency or a private contractor acting as an agent for the authorized receiving agency complies with the security and management control outsourcing standard for non-channelers (see Exhibit A).
10. NCJA is responsible for compliance to technical standards set forth by WSP and the CJIS Security Policy.
11. NCJA will conduct periodic self audits to ensure compliance with CJIS Security Policy.
12. NCJA will participate in WSP and FBI audits, provide plans for any compliance issues, and follow through to resolution within identified timeframes.
13. NCJA will ensure all appropriate staff members are trained according to the state and federal requirements.

### **III. CRIMINAL HISTORY RECORD INFORMATION RESPONSIBILITIES**

NCJA shall conform to system policies, as established by the FBI CJIS Division and WSP, before access to CHRI is permitted. This will allow for control over the data and give assurance of system security.

1. The rules and procedures governing access to CHRI shall apply equally to all participants in the system.
2. All noncriminal justice agencies with access to CHRI data must designate a specific unit, position, or personnel to access CHRI; noncriminal justice agencies must advise WSP of such personnel and changes to such designation.
3. All noncriminal justice agencies with access to CHRI data from the system shall permit an FBI CJIS Division or WSP audit team to conduct appropriate audits. NCJA must cooperate with these audits and respond promptly.

### **IV. SECURITY RESPONSIBILITIES**

#### **Technical Roles and Responsibilities**

NCJA must comply with and enforce system security. NCJA must have someone designated as the security point of contact (POC). Security POC's shall be responsible for the following:

1. Identifying the user of the hardware/software and ensuring that no unauthorized users have access to the same.
2. Identifying and documenting how the equipment is connected to the state system.

3. Ensuring that personnel security screening procedures are being followed as stated in the CJIS Security Policy.
4. Ensuring that appropriate hardware security measures are in place.
5. Supporting policy compliance and keeping the WSP informed of security incidents.
6. If the technical POC changes at your agency, notify WSP immediately.

#### **Security Enforcement**

NCJA is responsible for enforcing system security standards for their agency, in addition to all of the other agencies to which the NCJA provides CHRI information. Authorized users shall access and disseminate the CHRI data only for the purpose for which they are authorized. NCJA shall have a written policy for the discipline of policy violators.

#### **Technical Security Training**

All Information Technology (IT) employees who have access to and those who have direct responsibility to configure and maintain FBI CJIS systems must review security awareness training within six months of their appointment or assignment. Documentation pertaining to the materials used and those employees which receive security awareness training shall be maintained in a current status.

#### **Physical Security**

A physically secured location in a noncriminal justice facility, an area, a room, a group of rooms, that is/are subject to criminal justice agency management control security addendum and which contain hardware, software, and/or firmware (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch panels, etc.) that provide access to the CJIS sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that restrict unauthorized access.

All personnel with access to computer centers, CHRI, or areas where CHRI information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check. All personnel must review security awareness training within six months of their appointment or assignment.

#### **Personnel Security**

To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days of initial employment or assignment for all personnel who have authorized access to FBI CJIS information and those who have direct responsibility to configure and maintain computer systems and networks with access to FBI CJIS information. All requests from system access shall be made as specified by the CJIS Systems Officer (i.e. WSP Identification and Criminal History Section).

- c. NCJA shall use the data supplied by WSP and the FBI under this MOU only for the authorized purpose intended. NCJA shall not use this data for any other purpose and shall not disseminate this data with any other parties unless required by law. NCJA shall share any public disclosure requests regarding this data with the WSP.

#### **Storage**

Please see 'Security and Management Control Outsourcing Standard for Non-Channelers' (Exhibit A).



**V. LIAISON REPRESENTATIVES**

**For the Washington State Patrol:**

Jim Anderson, Administrator  
Criminal Records Division  
PO Box 42619  
Olympia WA 98504-2619  
Phone: (360) 534-2101  
Fax: (360) 534-2070  
E-mail: [jim.anderson@wsp.wa.gov](mailto:jim.anderson@wsp.wa.gov)

**For the Kitsap County Juvenile Court:**

Michael Mettinger  
1338 SW Old Clifton Rd  
Port Orchard WA 98366  
360-337-5410  
[dgicoso@co.kitsa.wa.us](mailto:dgicoso@co.kitsa.wa.us)

**VI. INDEMNIFICATION**

Each party shall defend, protect and hold harmless the other party from and against all claims, suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing this MOU.

**VII. PERIOD OF MOU**

This MOU becomes effective on the date of the last signature and continues for three years and may be renewed. It may be modified by mutual written consent of the two agencies. Liaison Representatives may modify Exhibit A by mutual written consent of the two agencies without changing the general conditions of this MOU.

**VIII. TERMINATION**

Except as otherwise provided in this MOU, either party may terminate this MOU upon ninety (90) days' written notification to the other party. If this MOU is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this MOU for performance prior to the effective date of termination.

**IX. DISPUTES**

In the event that a dispute arises under this MOU, it shall be determined in the following manner: The Chief of WSP, or designee, shall appoint one member to the Dispute Board. NCJA shall appoint one member to the Dispute Board. The Chief of WSP, or designee, and the NCJA shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. If applicable and as an alternative to this process, either of the parties may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.

**X. EXHIBITS**

The exhibits listed below are incorporated into and made a part of this MOU:

Exhibit A - 'Security and Management Control Outsourcing Standard for Non-Channelers'

Exhibit B - Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.2, published 8/9/2013 which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

**XI. ORDER OF PRECEDENCE**

In the event of any inconsistency in the terms of this MOU, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:


- a. Applicable federal and state statutes and regulations;
- b. The Terms and Conditions contained in this MOU;
- c. The Exhibits attached to this MOU;
- d. Any other provisions of the MOU, whether incorporated by reference or otherwise.

**XII. ALL WRITINGS CONTAINED HEREIN**

This MOU contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this MOU shall be deemed to exist or to bind any of the parties hereto.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

KITSAP COUNTY JUVENILE COURT

*fw*   
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_

2/15/14  
\_\_\_\_\_  
Date

12-20-13  
\_\_\_\_\_  
Date

## SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD for NON-CHANNELERS

The goal of this document is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the Contractor. Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security and Management Control Outsourcing Standard (Outsourcing Standard) is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI without a direct connection to the FBI CJIS Wide Area Network (WAN).

### 1.0 *Definitions*

- 1.01 *Access to CHRI* means to view or make use of CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by title 42, United States Code, section 14614(b).
- 1.02 *Authorized Recipient* means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.
- 1.03 *Chief Administrator* means the primary administrator of a Nonparty State’s criminal history record repository or a designee of such administrator who is

a regular full-time employee of the repository, which is also referred to as the State Identification Bureau (SIB) Chief.

- 1.04 *CHRI*, as referred to in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.
- 1.05 *Criminal History Record Check*, for purposes of this Outsourcing Standard only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.
- 1.06 *Compact Officer*, as provided in Article I(2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the compact among federal agencies], or (B) with respect to a Party State, the chief administrator of the State's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.
- 1.07 *Contractor* means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI.
- 1.08 *Dissemination* means the disclosure of CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 1.09 *Noncriminal Justice Administrative Functions* means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:
1. Making fitness determinations/recommendations
  2. Obtaining missing dispositions
  3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General
  4. Other authorized activities relating to the general handling, use, and storage of CHRI

- 1.10 *Noncriminal Justice Purposes*, as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.
- 1.11 *Outsourcing Standard* means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. This Outsourcing Standard authorizes access to CHRI for noncriminal justice purposes, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.
- 1.12 *Physically Secure Location* means a facility or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CHRI and associated information systems.
- 1.13 *Positive Identification*, as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints<sup>1</sup> or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other non-unique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.
- 1.14 *Public Carrier Network* means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: Dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.
- 1.15 *Security Violation* means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in

---

<sup>1</sup> The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning positive identification may be obtained from the FBI Compact Council office.

violation of: (A) Federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

2.0 *Responsibilities of the Authorized Recipient*

- 2.01 Prior to engaging in outsourcing any noncriminal justice administrative functions, the Authorized Recipient shall: (a) Request and receive written permission from (1) the State Compact Officer/Chief Administrator<sup>2</sup> or (2) the FBI Compact Officer<sup>3</sup>; (b) provide the Compact Officer/Chief Administrator copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested; and (c) inquire of the FBI Compact Officer whether a prospective Contractor has any security violations (See Section 8.04). The FBI Compact Officer will report those findings to the Authorized Recipient and, when applicable, to the State Compact Officer/Chief Administrator.
- 2.02 The Authorized Recipient shall execute a contract or agreement prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.
- 2.03 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; limit retention of the information to a period of time not to exceed that period of time the Authorized Recipient is permitted to retain such information; prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General; ensure the security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; and ensure that Contractor

---

<sup>2</sup>The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and Authorized Recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.

<sup>3</sup>State or local Authorized Recipients based on State or Federal Statutes shall contact the State Compact Officer/Chief Administrator. Federal or Regulatory Agency Authorized Recipients shall contact the FBI Compact Officer.

personnel comply with this Outsourcing Standard.

- a. The Authorized Recipient shall conduct criminal history record checks of Contractor personnel having access to CHRI if such checks are required or authorized of the Authorized Recipient's personnel having similar access.<sup>4</sup> The Authorized Recipient shall maintain updated records of Contractor personnel who have access to CHRI and update those records within 24 hours when changes to that access occur and, if a criminal history record check is required, the Authorized Recipient shall maintain a list of Contractor personnel who successfully completed the criminal history record check.
  - b. The Authorized Recipient shall ensure that the Contractor maintains site security.
  - c. The Authorized Recipient shall ensure that the most current version of both the Outsourcing Standard and the CJIS Security Policy are incorporated by reference at the time of contract, contract renewal, or within 30 calendar days (unless otherwise directed) of notification of successor versions of the Outsourcing Standard and/or CJIS Security Policy, whichever is sooner. The Authorized Recipient shall notify the Contractor within 30 calendar days (unless otherwise directed) of FBI notification regarding changes or updates to the Outsourcing Standard and/or CJIS Security Policy.
- 2.04 The Authorized Recipient shall understand the communications and record capabilities of the Contractor which has access to federal or state records through, or because of, its outsourcing relationship with the Authorized Recipient. The Authorized Recipient shall maintain an updated topological drawing which depicts the interconnectivity of the Contractor's network configuration.
- 2.05 The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the Outsourcing Standard. The Authorized Recipient shall certify to the Compact Officer/Chief Administrator that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.

---

<sup>4</sup>If a national criminal history record check of Authorized Recipient personnel having access to CHRI is mandated or authorized by a federal statute, executive order, or state statute approved by the Attorney General under Public Law 92-544, the State Compact Officer/Chief Administrator and/or the FBI Compact Officer must ensure Contractor personnel having similar access are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives. The national criminal history record checks of Contractor personnel with access to CHRI cannot be outsourced and must be performed by the Authorized Recipient.

2.06 The Authorized Recipient shall provide written notice of any early voluntary termination of the contract to the Compact Officer/Chief Administrator or the FBI Compact Officer.

3.0 *Responsibilities of the Contractor*

3.01 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the CJIS Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

3.02 The Contractor shall develop, document, administer, and maintain a Security Program (Physical, Personnel, and Information Technology) to comply with the most current Outsourcing Standard and the most current FBI *CJIS Security Policy*. The Security Program shall describe the implementation of the security requirements described in this Outsourcing Standard and the FBI *CJIS Security Policy*. In addition, the Contractor is also responsible to set, maintain, and enforce the standards for the selection, supervision, and separation of personnel who have access to CHRI. The Authorized Recipient shall provide the written approval of a Contractor's Security Program.

3.03 The requirements for a Security Program should include, at a minimum:

- a) Description of the implementation of the security requirements described in this Outsourcing Standard and the *CJIS Security Policy*.
- b) Security Training.
- c) Guidelines for documentation of security violations.
- d) Standards for the selection, supervision, and separation of personnel with access to CHRI.

\*\*If the Contractor is using a corporate policy, it must meet the requirements outlined in this Outsourcing Standard and the *CJIS Security Policy*. If the corporate policy is not this specific, it must flow down to a level where the documentation supports these requirements.

3.04 Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. The Authorized Recipient shall review and provide to the Contractor written approval of the Security Training Program. Training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall annually, not later than the anniversary date of the contract, certify in writing to the Authorized Recipient that annual refresher training was completed for those Contractor personnel with access



to CHRI.

- 3.05 The Contractor shall make its facilities available for announced and unannounced audits performed by the Authorized Recipient, the state, or the FBI on behalf of the Compact Council.
- 3.06 The Contractor's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI CJIS Division. During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.
- 3.07 The Contractor shall maintain CHRI only for the period of time necessary to fulfill its contractual obligations but not to exceed the period of time that the Authorized Recipient is authorized to maintain and does maintain the CHRI.
- 3.08 The Contractor shall maintain a log of any dissemination of CHRI, for a minimum of 365 days.

#### 4.0 *Site Security*

- 4.01 The Authorized Recipient shall ensure that the Contractor site(s) is a physically secure location to protect against any unauthorized access to CHRI.

#### 5.0 *Dissemination*

- 5.01 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 5.02 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) The Authorized Recipient and the secondary recipient with unique identifiers, (B) the record disseminated, (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.
- 5.03 If CHRI is stored or disseminated in an electronic format, the Contractor shall protect against unauthorized access to the equipment and any of the data. In no event shall responses containing CHRI be disseminated other than as governed by this Outsourcing Standard or more stringent contract requirements.

#### 6.0 *Personnel Security*

- 6.01 If a local, state, or federal written standard requires or authorizes a criminal history record check of the Authorized Recipient's personnel with access to

CHRI, then a criminal history record check shall be required of the Contractor's (and approved Sub-Contractor's) employees having access to CHRI. Criminal history record checks of Contractor and approved Sub-Contractor employees, at a minimum, will be no less stringent than criminal history record checks that are performed on the Authorized Recipient's personnel performing similar functions. Criminal history record checks must be completed prior to accessing CHRI under the contract.

- 6.02 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm in writing that each employee has certified in writing that he/she understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities. The Contractor shall maintain the employee certifications in a file that is subject to review during audits. Employees shall make such certification prior to performing work under the contract.
- 6.03 The Contractor shall maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur, and if a criminal history record check is required, maintain a list of personnel who have successfully completed criminal history record checks. The Contractor shall notify Authorized Recipients within 24 hours when additions or deletions occur.

## 7.0 *System Security*

- 7.01 The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy.
  - a. If CHRI can be accessed by unauthorized personnel via Wide Area Network/Local Area Network or the Internet, then the Contractor shall protect the CHRI with firewall-type devices to prevent such unauthorized access. These devices shall implement a minimum firewall profile as specified by the CJIS Security Policy in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.
  - b. Data encryption shall be required throughout the network passing CHRI through a shared public carrier network.
- 7.02 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.
  - a. CHRI shall be stored in a physically secure location.
  - b. The Authorized Recipient shall ensure that a procedure is in place for

sanitizing all fixed storage media (e.g., disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal, or reuse. Sanitization procedures include overwriting the media and/or degaussing the media.

- c. The Authorized Recipient shall ensure that a procedure is in place for the disposal or return of all non-fixed storage media (e.g., hard copies, print-outs).

7.03 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient, Contractor, or sub-Contractor must be assigned a unique identifying number.

## 8.0 *Security Violations*

### 8.01 Duties of the Authorized Recipient and Contractor

- a. The Contractor shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference.
- b. Pending investigation, the Contractor shall, upon detection or awareness, suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.
- c. The Contractor shall immediately (within four hours) notify the Authorized Recipient of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. Within five calendar days of such notification, the Contractor shall provide the Authorized Recipient a written report documenting such security violation, any corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.
- d. The Authorized Recipient shall immediately (within four hours) notify the State Compact Officer/Chief Administrator and the FBI Compact Officer of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator, if applicable, and the FBI Compact Officer, within five calendar days of receipt of the written report from the Contractor. The written report must include any corrective actions taken by the Contractor and the Authorized Recipient to resolve such security violation.

- 8.02 Termination of the contract by the Authorized Recipient for security violations
- a. The contract is subject to termination by the Authorized Recipient for security violations involving CHRI obtained pursuant to the contract.
  - b. The contract is subject to termination by the Authorized Recipient for the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.
  - c. If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient shall terminate the contract.
- 8.03 Suspension or termination of the exchange of CHRI for security violations
- a. Notwithstanding the actions taken by the State Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Compact Council or the United States Attorney General may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 CFR §906.2(d).
  - b. If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United States Attorney General by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be deleted or returned in accordance with the provisions and time frame as specified by the Authorized Recipient.
- 8.04 The Authorized Recipient shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following:
- a. The termination of a contract for security violations.
  - b. Security violations involving the unauthorized access to CHRI.
  - c. The Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.
- 8.05 The Compact Officer/Chief Administrator, Compact Council and the United States Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.
- 8.06 The Compact Officer/Chief Administrator, Compact Council, and the United

States Attorney General reserve the right to audit the Authorized Recipient and the Contractor's operations and procedures at scheduled or unscheduled times. The Compact Council, the United States Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the contract.

9.0 *Miscellaneous Provisions*

- 9.01 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, Compact Officer/Chief Administrator (where applicable), and the FBI.
- 9.02 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) The CJIS Security Policy.
- 9.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and the CHRI accessed therefrom and it is understood that there may be terms and conditions of the appended contract which impose more stringent requirements upon the Contractor.<sup>5</sup>
- 9.04 The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. Conformance to such security measures may not be less stringent than stated in this Outsourcing Standard without the consent of the Compact Council in consultation with the United States Attorney General.
- 9.05 This Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.
- 9.06 Appropriate notices, assurances, and correspondence to the FBI Compact Officer, Compact Council, and the United States Attorney General required by Section 8.0 of this Outsourcing Standard shall be forwarded by First Class Mail to:
  - FBI Compact Officer
  - 1000 Custer Hollow Road
  - Module D-3
  - Clarksburg, WV 26306

10.0 *Exemption from Above Provisions*

---

<sup>5</sup>Such conditions could include additional audits, fees, or security requirements. The Compact Council, Authorized Recipients, and the Compact Officer/Chief Administrator have the explicit authority to require more stringent standards than those contained in the Outsourcing Standard.

- 10.01 An Information Technology (IT) contract need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:
1. Access to CHRI by the IT contractor's personnel is limited solely for the development and/or maintenance of the Authorized Recipient's computer system;
  2. Access to CHRI is incidental, but necessary, to the duties being performed by the IT contractor;
  3. The computer system resides within the Authorized Recipient's facility;
  4. The Authorized Recipient's personnel supervise or work directly with the IT contractor personnel;
  5. The Authorized Recipient maintains complete, positive control of the IT contractor's access to the computer system and CHRI contained therein; and
  6. The Authorized Recipient retains all of the duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard.

10.02 An Authorized Recipient's contract where access to CHRI is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 4.0, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:

1. Access to CHRI by the Contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient;
2. Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor;

3. The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the Authorized Recipient;
4. The Contractor's personnel are subject to the same criminal history record checks as the Authorized Recipient's personnel;
5. The criminal history record checks of the Contractor personnel are completed prior to work on the contract or agreement;
6. The Authorized Recipient retains all other duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard; and
7. The Contractor stores the CHRI in a physically secure location.

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above referenced Contract between the Washington State Patrol and the Kitsap County Juvenile Court is hereby amended as follows:

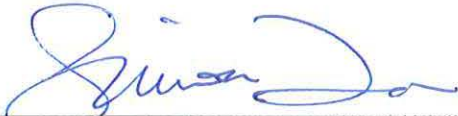
- The end date shall be extended through February 4, 2022.
- **Exhibit B** "CJIS Security Policy" shall be replaced by **Exhibit B** – Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.5, published 6/1/2016 which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

KITSAP COUNTY JUVENILE COURT



FOR: John R. Batiste, Chief



Signature

4-14-17

Date

4-10-17

Date



**MEMORANDUM OF UNDERSTANDING**

**Between the**

**WASHINGTON STATE PATROL**

**And the**

**KITTITAS COUNTY SUPERIOR COURT**

**I. PURPOSE**

The parties to this Memorandum of Understanding (MOU) are the Washington State Patrol, Identification and Criminal History Section (WSP) and the Kittitas County Superior Court, a non criminal justice agency (NCJA). This MOU sets forth the policy to ensure the protection of criminal history record information (CHRI) between the WSP, the NCJA, and the Federal Bureau of Investigation (FBI). This MOU provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CHRI data. This policy applies to the NCJA and its contractors with access to, or who operate in support of, non-criminal justice services and information.

**II. ADMINISTRATIVE RESPONSIBILITIES**

As participants in this MOU, the parties will develop mutually and separately appropriate procedures for transmission, dissemination, storage, and destruction of CHRI data.

- a. The Washington State Patrol. WSP shall ensure the NCJA complies with the Criminal Justice Information Services (CJIS) Security Policy (See Exhibit B) which includes authorized use of CHRI, dissemination of CHRI, statute authorization for civil applicant background checks conducted by noncriminal justice agencies, applicant notification and record challenge, security of CHRI, storage of CHRI, outsourcing of noncriminal justice administrative functions, and user fees. WSP will conduct regional audits of all agencies working under this MOU to ensure compliance to all state and federal standards.
- b. NCJA. The NCJA shall be responsible for ensuring:
  1. NCJA responds to requests for information by the FBI CJIS Division or the WSP in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of the agency.
  2. NCJA has formalized written procedures for the following, if applicable: criminal history use and dissemination, misuse, background checks, password management, storage, and destruction of CHRI.
  3. CHRI received as a result of licensing or employment purposes, pursuant to Public Law 92-544 is solely used for the purpose for which the record was requested. Subject fingerprints shall be submitted with all requests for CHRI for noncriminal justice purposes. Access to the FBI CJIS using name-based inquiry and record request messages is not permitted for noncriminal justice purpose, unless otherwise approved by the FBI.
  4. Access to CHRI by authorized officials is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or other authorized entities.

5. All fingerprint based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.
6. NCJA must notify the applicants fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The officials making the determination of suitability for licensing or employment shall provide the applicants the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record. These officials also must advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in Title 28, C.F.R. 16.34. Official making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so.
7. Appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity.
8. NCJA shall seek WSP permission prior to outsourcing noncriminal justice functions.
9. Outsourcing of noncriminal justice administrative functions requiring access to CHRI to either another governmental agency or a private contractor acting as an agent for the authorized receiving agency complies with the security and management control outsourcing standard for non-channelers (see Exhibit A).
10. NCJA is responsible for compliance to technical standards set forth by WSP and the CJIS Security Policy.
11. NCJA will conduct periodic self audits to ensure compliance with CJIS Security Policy.
12. NCJA will participate in WSP and FBI audits, provide plans for any compliance issues, and follow through to resolution within identified timeframes.
13. NCJA will ensure all appropriate staff members are trained according to the state and federal requirements.

### **III. CRIMINAL HISTORY RECORD INFORMATION RESPONSIBILITIES**

NCJA shall conform to system policies, as established by the FBI CJIS Division and WSP, before access to CHRI is permitted. This will allow for control over the data and give assurance of system security.

1. The rules and procedures governing access to CHRI shall apply equally to all participants in the system.
2. All noncriminal justice agencies with access to CHRI data must designate a specific unit, position, or personnel to access CHRI; noncriminal justice agencies must advise WSP of such personnel and changes to such designation.
3. All noncriminal justice agencies with access to CHRI data from the system shall permit an FBI CJIS Division or WSP audit team to conduct appropriate audits. NCJA must cooperate with these audits and respond promptly.

### **IV. SECURITY RESPONSIBILITIES**

#### **Technical Roles and Responsibilities**

NCJA must comply with and enforce system security. NCJA must have someone designated as the security point of contact (POC). Security POC's shall be responsible for the following:

1. Identifying the user of the hardware/software and ensuring that no unauthorized users have access to the same.
2. Identifying and documenting how the equipment is connected to the state system.

3. Ensuring that personnel security screening procedures are being followed as stated in the CJIS Security Policy.
4. Ensuring that appropriate hardware security measures are in place.
5. Supporting policy compliance and keeping the WSP informed of security incidents.
6. If the technical POC changes at your agency, notify WSP immediately.

#### **Security Enforcement**

NCJA is responsible for enforcing system security standards for their agency, in addition to all of the other agencies to which the NCJA provides CHRI information. Authorized users shall access and disseminate the CHRI data only for the purpose for which they are authorized. NCJA shall have a written policy for the discipline of policy violators.

#### **Technical Security Training**

All Information Technology (IT) employees who have access to and those who have direct responsibility to configure and maintain FBI CJIS systems must review security awareness training within six months of their appointment or assignment. Documentation pertaining to the materials used and those employees which receive security awareness training shall be maintained in a current status.

#### **Physical Security**

A physically secured location in a noncriminal justice facility, an area, a room, a group of rooms, that is/are subject to criminal justice agency management control security addendum and which contain hardware, software, and/or firmware (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch panels, etc.) that provide access to the CJIS sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that restrict unauthorized access.

All personnel with access to computer centers, CHRI, or areas where CHRI information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check. All personnel must review security awareness training within six months of their appointment or assignment.

#### **Personnel Security**

To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days of initial employment or assignment for all personnel who have authorized access to FBI CJIS information and those who have direct responsibility to configure and maintain computer systems and networks with access to FBI CJIS information. All requests from system access shall be made as specified by the CJIS Systems Officer (i.e. WSP Identification and Criminal History Section).

- c. NCJA shall use the data supplied by WSP and the FBI under this MOU only for the authorized purpose intended. NCJA shall not use this data for any other purpose and shall not disseminate this data with any other parties unless required by law. NCJA shall share any public disclosure requests regarding this data with the WSP.

#### **Storage**

Please see 'Security and Management Control Outsourcing Standard for Non-Channelers' (Exhibit A).

**V. LIAISON REPRESENTATIVES**

**For the Washington State Patrol:**

Jim Anderson, Administrator  
Criminal Records Division  
PO Box 42619  
Olympia WA 98504-2619  
Phone: (360) 534-2101  
Fax: (360) 534-2070  
E-mail: [jim.anderson@wsp.wa.gov](mailto:jim.anderson@wsp.wa.gov)

**For the Kittitas County Superior Court:**

Anna Barnaby  
205 W 5th Ste 207  
Ellensburg WA 98926  
509-962-7533  
[anna.barnaby@co.kittitas.wa.us](mailto:anna.barnaby@co.kittitas.wa.us)

**VI. INDEMNIFICATION**

Each party shall defend, protect and hold harmless the other party from and against all claims, suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing this MOU.

**VII. PERIOD OF MOU**

This MOU becomes effective on the date of the last signature and continues for three years and may be renewed. It may be modified by mutual written consent of the two agencies. Liaison Representatives may modify Exhibit A by mutual written consent of the two agencies without changing the general conditions of this MOU.

**VIII. TERMINATION**

Except as otherwise provided in this MOU, either party may terminate this MOU upon ninety (90) days' written notification to the other party. If this MOU is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this MOU for performance prior to the effective date of termination.

**IX. DISPUTES**

In the event that a dispute arises under this MOU, it shall be determined in the following manner: The Chief of WSP, or designee, shall appoint one member to the Dispute Board. NCJA shall appoint one member to the Dispute Board. The Chief of WSP, or designee, and the NCJA shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. If applicable and as an alternative to this process, either of the parties may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.

**X. EXHIBITS**

The exhibits listed below are incorporated into and made a part of this MOU:

Exhibit A - 'Security and Management Control Outsourcing Standard for Non-Channelers'

Exhibit B - Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.2, published 8/9/2013 which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

**XI. ORDER OF PRECEDENCE**

In the event of any inconsistency in the terms of this MOU, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

- a. Applicable federal and state statutes and regulations;
- b. The Terms and Conditions contained in this MOU;
- c. The Exhibits attached to this MOU;
- d. Any other provisions of the MOU, whether incorporated by reference or otherwise.

**XII. ALL WRITINGS CONTAINED HEREIN**

This MOU contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this MOU shall be deemed to exist or to bind any of the parties hereto.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

KITTITAS COUNTY SUPERIOR COURT

  
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_

Date

9/26/13

Date

9-19-13

## SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD for NON-CHANNELERS

The goal of this document is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the Contractor. Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security and Management Control Outsourcing Standard (Outsourcing Standard) is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI without a direct connection to the FBI CJIS Wide Area Network (WAN).

### 1.0 *Definitions*

- 1.01 *Access to CHRI* means to view or make use of CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by title 42, United States Code, section 14614(b).
- 1.02 *Authorized Recipient* means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.
- 1.03 *Chief Administrator* means the primary administrator of a Nonparty State’s criminal history record repository or a designee of such administrator who is

a regular full-time employee of the repository, which is also referred to as the State Identification Bureau (SIB) Chief.

- 1.04 *CHRI*, as referred to in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.
- 1.05 *Criminal History Record Check*, for purposes of this Outsourcing Standard only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.
- 1.06 *Compact Officer*, as provided in Article I(2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the compact among federal agencies], or (B) with respect to a Party State, the chief administrator of the State's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.
- 1.07 *Contractor* means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI.
- 1.08 *Dissemination* means the disclosure of CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 1.09 *Noncriminal Justice Administrative Functions* means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:
1. Making fitness determinations/recommendations
  2. Obtaining missing dispositions
  3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General
  4. Other authorized activities relating to the general handling, use, and storage of CHRI

- 1.10 *Noncriminal Justice Purposes*, as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.
- 1.11 *Outsourcing Standard* means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. This Outsourcing Standard authorizes access to CHRI for noncriminal justice purposes, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.
- 1.12 *Physically Secure Location* means a facility or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CHRI and associated information systems.
- 1.13 *Positive Identification*, as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints<sup>1</sup> or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other non-unique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.
- 1.14 *Public Carrier Network* means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: Dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.
- 1.15 *Security Violation* means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in

---

<sup>1</sup> The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning positive identification may be obtained from the FBI Compact Council office.



violation of: (A) Federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

2.0 *Responsibilities of the Authorized Recipient*

- 2.01 Prior to engaging in outsourcing any noncriminal justice administrative functions, the Authorized Recipient shall: (a) Request and receive written permission from (1) the State Compact Officer/Chief Administrator<sup>2</sup> or (2) the FBI Compact Officer<sup>3</sup>; (b) provide the Compact Officer/Chief Administrator copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested; and (c) inquire of the FBI Compact Officer whether a prospective Contractor has any security violations (See Section 8.04). The FBI Compact Officer will report those findings to the Authorized Recipient and, when applicable, to the State Compact Officer/Chief Administrator.
- 2.02 The Authorized Recipient shall execute a contract or agreement prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.
- 2.03 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; limit retention of the information to a period of time not to exceed that period of time the Authorized Recipient is permitted to retain such information; prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General; ensure the security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; and ensure that Contractor

---

<sup>2</sup>The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and Authorized Recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.

<sup>3</sup>State or local Authorized Recipients based on State or Federal Statutes shall contact the State Compact Officer/Chief Administrator. Federal or Regulatory Agency Authorized Recipients shall contact the FBI Compact Officer.

personnel comply with this Outsourcing Standard.

- a. The Authorized Recipient shall conduct criminal history record checks of Contractor personnel having access to CHRI if such checks are required or authorized of the Authorized Recipient's personnel having similar access.<sup>4</sup> The Authorized Recipient shall maintain updated records of Contractor personnel who have access to CHRI and update those records within 24 hours when changes to that access occur and, if a criminal history record check is required, the Authorized Recipient shall maintain a list of Contractor personnel who successfully completed the criminal history record check.
  - b. The Authorized Recipient shall ensure that the Contractor maintains site security.
  - c. The Authorized Recipient shall ensure that the most current version of both the Outsourcing Standard and the CJIS Security Policy are incorporated by reference at the time of contract, contract renewal, or within 30 calendar days (unless otherwise directed) of notification of successor versions of the Outsourcing Standard and/or CJIS Security Policy, whichever is sooner. The Authorized Recipient shall notify the Contractor within 30 calendar days (unless otherwise directed) of FBI notification regarding changes or updates to the Outsourcing Standard and/or CJIS Security Policy.
- 2.04 The Authorized Recipient shall understand the communications and record capabilities of the Contractor which has access to federal or state records through, or because of, its outsourcing relationship with the Authorized Recipient. The Authorized Recipient shall maintain an updated topological drawing which depicts the interconnectivity of the Contractor's network configuration.
- 2.05 The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the Outsourcing Standard. The Authorized Recipient shall certify to the Compact Officer/Chief Administrator that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.

---

<sup>4</sup>If a national criminal history record check of Authorized Recipient personnel having access to CHRI is mandated or authorized by a federal statute, executive order, or state statute approved by the Attorney General under Public Law 92-544, the State Compact Officer/Chief Administrator and/or the FBI Compact Officer must ensure Contractor personnel having similar access are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives. The national criminal history record checks of Contractor personnel with access to CHRI cannot be outsourced and must be performed by the Authorized Recipient.

2.06 The Authorized Recipient shall provide written notice of any early voluntary termination of the contract to the Compact Officer/Chief Administrator or the FBI Compact Officer.

3.0 *Responsibilities of the Contractor*

3.01 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the CJIS Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

3.02 The Contractor shall develop, document, administer, and maintain a Security Program (Physical, Personnel, and Information Technology) to comply with the most current Outsourcing Standard and the most current FBI *CJIS Security Policy*. The Security Program shall describe the implementation of the security requirements described in this Outsourcing Standard and the FBI *CJIS Security Policy*. In addition, the Contractor is also responsible to set, maintain, and enforce the standards for the selection, supervision, and separation of personnel who have access to CHRI. The Authorized Recipient shall provide the written approval of a Contractor's Security Program.

3.03 The requirements for a Security Program should include, at a minimum:

- a) Description of the implementation of the security requirements described in this Outsourcing Standard and the *CJIS Security Policy*.
- b) Security Training.
- c) Guidelines for documentation of security violations.
- d) Standards for the selection, supervision, and separation of personnel with access to CHRI.

*\*\*If the Contractor is using a corporate policy, it must meet the requirements outlined in this Outsourcing Standard and the *CJIS Security Policy*. If the corporate policy is not this specific, it must flow down to a level where the documentation supports these requirements.*

3.04 Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. The Authorized Recipient shall review and provide to the Contractor written approval of the Security Training Program. Training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall annually, not later than the anniversary date of the contract, certify in writing to the Authorized Recipient that annual refresher training was completed for those Contractor personnel with access

to CHRI.

- 3.05 The Contractor shall make its facilities available for announced and unannounced audits performed by the Authorized Recipient, the state, or the FBI on behalf of the Compact Council.
- 3.06 The Contractor's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI CJIS Division. During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.
- 3.07 The Contractor shall maintain CHRI only for the period of time necessary to fulfill its contractual obligations but not to exceed the period of time that the Authorized Recipient is authorized to maintain and does maintain the CHRI.
- 3.08 The Contractor shall maintain a log of any dissemination of CHRI, for a minimum of 365 days.

#### 4.0 *Site Security*

- 4.01 The Authorized Recipient shall ensure that the Contractor site(s) is a physically secure location to protect against any unauthorized access to CHRI.

#### 5.0 *Dissemination*

- 5.01 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 5.02 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) The Authorized Recipient and the secondary recipient with unique identifiers, (B) the record disseminated, (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.
- 5.03 If CHRI is stored or disseminated in an electronic format, the Contractor shall protect against unauthorized access to the equipment and any of the data. In no event shall responses containing CHRI be disseminated other than as governed by this Outsourcing Standard or more stringent contract requirements.

#### 6.0 *Personnel Security*

- 6.01 If a local, state, or federal written standard requires or authorizes a criminal history record check of the Authorized Recipient's personnel with access to

CHRI, then a criminal history record check shall be required of the Contractor's (and approved Sub-Contractor's) employees having access to CHRI. Criminal history record checks of Contractor and approved Sub-Contractor employees, at a minimum, will be no less stringent than criminal history record checks that are performed on the Authorized Recipient's personnel performing similar functions. Criminal history record checks must be completed prior to accessing CHRI under the contract.

- 6.02 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm in writing that each employee has certified in writing that he/she understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities. The Contractor shall maintain the employee certifications in a file that is subject to review during audits. Employees shall make such certification prior to performing work under the contract.
- 6.03 The Contractor shall maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur, and if a criminal history record check is required, maintain a list of personnel who have successfully completed criminal history record checks. The Contractor shall notify Authorized Recipients within 24 hours when additions or deletions occur.

## 7.0 *System Security*

- 7.01 The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy.
  - a. If CHRI can be accessed by unauthorized personnel via Wide Area Network/Local Area Network or the Internet, then the Contractor shall protect the CHRI with firewall-type devices to prevent such unauthorized access. These devices shall implement a minimum firewall profile as specified by the CJIS Security Policy in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.
  - b. Data encryption shall be required throughout the network passing CHRI through a shared public carrier network.
- 7.02 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.
  - a. CHRI shall be stored in a physically secure location.
  - b. The Authorized Recipient shall ensure that a procedure is in place for

sanitizing all fixed storage media (e.g., disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal, or reuse. Sanitization procedures include overwriting the media and/or degaussing the media.

- c. The Authorized Recipient shall ensure that a procedure is in place for the disposal or return of all non-fixed storage media (e.g., hard copies, print-outs).

7.03 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient, Contractor, or sub-Contractor must be assigned a unique identifying number.

## 8.0 *Security Violations*

### 8.01 Duties of the Authorized Recipient and Contractor

- a. The Contractor shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference.
- b. Pending investigation, the Contractor shall, upon detection or awareness, suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.
- c. The Contractor shall immediately (within four hours) notify the Authorized Recipient of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. Within five calendar days of such notification, the Contractor shall provide the Authorized Recipient a written report documenting such security violation, any corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.
- d. The Authorized Recipient shall immediately (within four hours) notify the State Compact Officer/Chief Administrator and the FBI Compact Officer of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator, if applicable, and the FBI Compact Officer, within five calendar days of receipt of the written report from the Contractor. The written report must include any corrective actions taken by the Contractor and the Authorized Recipient to resolve such security violation.

- 8.02 Termination of the contract by the Authorized Recipient for security violations
  - a. The contract is subject to termination by the Authorized Recipient for security violations involving CHRI obtained pursuant to the contract.
  - b. The contract is subject to termination by the Authorized Recipient for the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.
  - c. If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient shall terminate the contract.
- 8.03 Suspension or termination of the exchange of CHRI for security violations
  - a. Notwithstanding the actions taken by the State Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Compact Council or the United States Attorney General may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 CFR §906.2(d).
  - b. If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United States Attorney General by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be deleted or returned in accordance with the provisions and time frame as specified by the Authorized Recipient.
- 8.04 The Authorized Recipient shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following:
  - a. The termination of a contract for security violations.
  - b. Security violations involving the unauthorized access to CHRI.
  - c. The Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.
- 8.05 The Compact Officer/Chief Administrator, Compact Council and the United States Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.
- 8.06 The Compact Officer/Chief Administrator, Compact Council, and the United

States Attorney General reserve the right to audit the Authorized Recipient and the Contractor's operations and procedures at scheduled or unscheduled times. The Compact Council, the United States Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the contract.

9.0 *Miscellaneous Provisions*

- 9.01 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, Compact Officer/Chief Administrator (where applicable), and the FBI.
- 9.02 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) The CJIS Security Policy.
- 9.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and the CHRI accessed therefrom and it is understood that there may be terms and conditions of the appended contract which impose more stringent requirements upon the Contractor.<sup>5</sup>
- 9.04 The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. Conformance to such security measures may not be less stringent than stated in this Outsourcing Standard without the consent of the Compact Council in consultation with the United States Attorney General.
- 9.05 This Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.
- 9.06 Appropriate notices, assurances, and correspondence to the FBI Compact Officer, Compact Council, and the United States Attorney General required by Section 8.0 of this Outsourcing Standard shall be forwarded by First Class Mail to:

FBI Compact Officer  
1000 Custer Hollow Road  
Module D-3  
Clarksburg, WV 26306

10.0 *Exemption from Above Provisions*

---

<sup>5</sup>Such conditions could include additional audits, fees, or security requirements. The Compact Council, Authorized Recipients, and the Compact Officer/Chief Administrator have the explicit authority to require more stringent standards than those contained in the Outsourcing Standard.



- 10.01 An Information Technology (IT) contract need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:
1. Access to CHRI by the IT contractor's personnel is limited solely for the development and/or maintenance of the Authorized Recipient's computer system;
  2. Access to CHRI is incidental, but necessary, to the duties being performed by the IT contractor;
  3. The computer system resides within the Authorized Recipient's facility;
  4. The Authorized Recipient's personnel supervise or work directly with the IT contractor personnel;
  5. The Authorized Recipient maintains complete, positive control of the IT contractor's access to the computer system and CHRI contained therein; and
  6. The Authorized Recipient retains all of the duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard.

10.02 An Authorized Recipient's contract where access to CHRI is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 4.0, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:

1. Access to CHRI by the Contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient;
2. Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor;

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above referenced Contract between the Washington State Patrol and the Kittitas County Superior Court is hereby amended as follows:

- The end date shall be extended through September 25, 2021.
- EXHIBIT B CJIS Security Policy 5.1 shall be replaced with EXHIBIT B CJIS Security Policy 5.5.

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL



FOR: John R. Batiste, Chief

2-3-2017

Date

KITTITAS COUNTY SUPERIOR COURT



Signature

Date

**MEMORANDUM OF UNDERSTANDING**

**Between the**

**WASHINGTON STATE PATROL**

**And the**

**PASCO POLICE DEPARTMENT**

**I. PURPOSE**

The parties to this Memorandum of Understanding (MOU) are the Washington State Patrol, Identification and Criminal History Section (WSP) and the Pasco Police Department, a non criminal justice agency (NCJA). This MOU sets forth the policy to ensure the protection of criminal history record information (CHRI) between the WSP, the NCJA, and the Federal Bureau of Investigation (FBI). This MOU provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CHRI data. This policy applies to the NCJA and its contractors with access to, or who operate in support of, non-criminal justice services and information.

**II. ADMINISTRATIVE RESPONSIBILITIES**

As participants in this MOU, the parties will develop mutually and separately appropriate procedures for transmission, dissemination, storage, and destruction of CHRI data.

- a. The Washington State Patrol. WSP shall ensure the NCJA complies with the Criminal Justice Information Services (CJIS) Security Policy (See Exhibit B) which includes authorized use of CHRI, dissemination of CHRI, statute authorization for civil applicant background checks conducted by noncriminal justice agencies, applicant notification and record challenge, security of CHRI, storage of CHRI, outsourcing of noncriminal justice administrative functions, and user fees. WSP will conduct regional audits of all agencies working under this MOU to ensure compliance to all state and federal standards.
- b. NCJA. The NCJA shall be responsible for ensuring:
  1. NCJA responds to requests for information by the FBI CJIS Division or the WSP in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of the agency.
  2. NCJA has formalized written procedures for the following, if applicable: criminal history use and dissemination, misuse, background checks, password management, storage, and destruction of CHRI.
  3. CHRI received as a result of licensing or employment purposes, pursuant to Public Law 92-544 is solely used for the purpose for which the record was requested. Subject fingerprints shall be submitted with all requests for CHRI for noncriminal justice purposes. Access to the FBI CJIS using name-based inquiry and record request messages is not permitted for noncriminal justice purpose, unless otherwise approved by the FBI.
  4. Access to CHRI by authorized officials is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or other authorized entities.

5. All fingerprint based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.
6. NCJA must notify the applicants fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The officials making the determination of suitability for licensing or employment shall provide the applicants the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record. These officials also must advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in Title 28, C.F.R. 16.34. Official making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so.
7. Appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity.
8. NCJA shall seek WSP permission prior to outsourcing noncriminal justice functions.
9. Outsourcing of noncriminal justice administrative functions requiring access to CHRI to either another governmental agency or a private contractor acting as an agent for the authorized receiving agency complies with the security and management control outsourcing standard for non-channelers (see Exhibit A).
10. NCJA is responsible for compliance to technical standards set forth by WSP and the CJIS Security Policy.
11. NCJA will conduct periodic self audits to ensure compliance with CJIS Security Policy.
12. NCJA will participate in WSP and FBI audits, provide plans for any compliance issues, and follow through to resolution within identified timeframes.
13. NCJA will ensure all appropriate staff members are trained according to the state and federal requirements.

### **III. CRIMINAL HISTORY RECORD INFORMATION RESPONSIBILITIES**

NCJA shall conform to system policies, as established by the FBI CJIS Division and WSP, before access to CHRI is permitted. This will allow for control over the data and give assurance of system security.

1. The rules and procedures governing access to CHRI shall apply equally to all participants in the system.
2. All noncriminal justice agencies with access to CHRI data must designate a specific unit, position, or personnel to access CHRI; noncriminal justice agencies must advise WSP of such personnel and changes to such designation.
3. All noncriminal justice agencies with access to CHRI data from the system shall permit an FBI CJIS Division or WSP audit team to conduct appropriate audits. NCJA must cooperate with these audits and respond promptly.

### **IV. SECURITY RESPONSIBILITIES**

#### **Technical Roles and Responsibilities**

NCJA must comply with and enforce system security. NCJA must have someone designated as the security point of contact (POC). Security POC's shall be responsible for the following:

1. Identifying the user of the hardware/software and ensuring that no unauthorized users have access to the same.
2. Identifying and documenting how the equipment is connected to the state system.

3. Ensuring that personnel security screening procedures are being followed as stated in the CJIS Security Policy.
4. Ensuring that appropriate hardware security measures are in place.
5. Supporting policy compliance and keeping the WSP informed of security incidents.
6. If the technical POC changes at your agency, notify WSP immediately.

### **Security Enforcement**

NCJA is responsible for enforcing system security standards for their agency, in addition to all of the other agencies to which the NCJA provides CHRI information. Authorized users shall access and disseminate the CHRI data only for the purpose for which they are authorized. NCJA shall have a written policy for the discipline of policy violators.

### **Technical Security Training**

All Information Technology (IT) employees who have access to and those who have direct responsibility to configure and maintain FBI CJIS systems must review security awareness training within six months of their appointment or assignment. Documentation pertaining to the materials used and those employees which receive security awareness training shall be maintained in a current status.

### **Physical Security**

A physically secured location in a noncriminal justice facility, an area, a room, a group of rooms, that is/are subject to criminal justice agency management control security addendum and which contain hardware, software, and/or firmware (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch panels, etc.) that provide access to the CJIS sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that restrict unauthorized access.

All personnel with access to computer centers, CHRI, or areas where CHRI information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check. All personnel must review security awareness training within six months of their appointment or assignment.

### **Personnel Security**

To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days of initial employment or assignment for all personnel who have authorized access to FBI CJIS information and those who have direct responsibility to configure and maintain computer systems and networks with access to FBI CJIS information. All requests from system access shall be made as specified by the CJIS Systems Officer (i.e. WSP Identification and Criminal History Section).

- c. NCJA shall use the data supplied by WSP and the FBI under this MOU only for the authorized purpose intended. NCJA shall not use this data for any other purpose and shall not disseminate this data with any other parties unless required by law. NCJA shall share any public disclosure requests regarding this data with the WSP.

### **Storage**

Please see 'Security and Management Control Outsourcing Standard for Non-Channelers' (Exhibit A).

**V. LIAISON REPRESENTATIVES**

**For the Washington State Patrol:**

Jim Anderson, Administrator  
Criminal Records Division  
PO Box 42619  
Olympia WA 98504-2619  
Phone: (360) 534-2101  
Fax:(360) 534-2070  
E-mail: [jim.anderson@wsp.wa.gov](mailto:jim.anderson@wsp.wa.gov)

**For the Pasco Police Department:**

Peggy Dvorak  
525 N 3rd Ave  
Pasco WA 99301  
509-545-3413  
[dvorakp@pasco-wa.gov](mailto:dvorakp@pasco-wa.gov)

**VI. INDEMNIFICATION**

Each party shall defend, protect and hold harmless the other party from and against all claims, suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing this MOU.

**VII. PERIOD OF MOU**

This MOU becomes effective on the date of the last signature and continues for three years and may be renewed. It may be modified by mutual written consent of the two agencies. Liaison Representatives may modify Exhibit A by mutual written consent of the two agencies without changing the general conditions of this MOU.

**VIII. TERMINATION**

Except as otherwise provided in this MOU, either party may terminate this MOU upon ninety (90) days' written notification to the other party. If this MOU is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this MOU for performance prior to the effective date of termination.

**IX. DISPUTES**

In the event that a dispute arises under this MOU, it shall be determined in the following manner: The Chief of WSP, or designee, shall appoint one member to the Dispute Board. NCJA shall appoint one member to the Dispute Board. The Chief of WSP, or designee, and the NCJA shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. If applicable and as an alternative to this process, either of the parties may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.

**X. EXHIBITS**

The exhibits listed below are incorporated into and made a part of this MOU:

Exhibit A - 'Security and Management Control Outsourcing Standard for Non-Channelers'

Exhibit B - Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.2, published 8/9/2013 which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

**XI. ORDER OF PRECEDENCE**

In the event of any inconsistency in the terms of this MOU, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

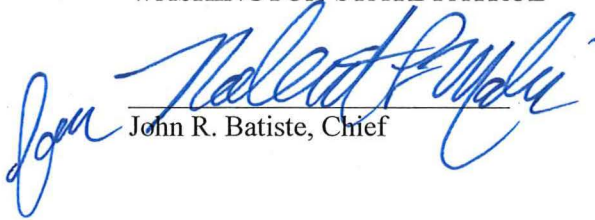
- a. Applicable federal and state statutes and regulations;
- b. The Terms and Conditions contained in this MOU;
- c. The Exhibits attached to this MOU;
- d. Any other provisions of the MOU, whether incorporated by reference or otherwise.

**XII. ALL WRITINGS CONTAINED HEREIN**

This MOU contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this MOU shall be deemed to exist or to bind any of the parties hereto.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

PASCO POLICE DEPARTMENT

  
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_  
POLICE CHIEF

\_\_\_\_\_  
Date

9-13-13  
\_\_\_\_\_  
Date

## SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD for NON-CHANNELERS

The goal of this document is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the Contractor. Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security and Management Control Outsourcing Standard (Outsourcing Standard) is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI without a direct connection to the FBI CJIS Wide Area Network (WAN).

### 1.0 *Definitions*

- 1.01 *Access to CHRI* means to view or make use of CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by title 42, United States Code, section 14614(b).
- 1.02 *Authorized Recipient* means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.
- 1.03 *Chief Administrator* means the primary administrator of a Nonparty State’s criminal history record repository or a designee of such administrator who is



a regular full-time employee of the repository, which is also referred to as the State Identification Bureau (SIB) Chief.

- 1.04 *CHRI*, as referred to in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.
- 1.05 *Criminal History Record Check*, for purposes of this Outsourcing Standard only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.
- 1.06 *Compact Officer*, as provided in Article I(2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the compact among federal agencies], or (B) with respect to a Party State, the chief administrator of the State's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.
- 1.07 *Contractor* means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI.
- 1.08 *Dissemination* means the disclosure of CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 1.09 *Noncriminal Justice Administrative Functions* means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:
1. Making fitness determinations/recommendations
  2. Obtaining missing dispositions
  3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General
  4. Other authorized activities relating to the general handling, use, and storage of CHRI

- 1.10 *Noncriminal Justice Purposes*, as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.
- 1.11 *Outsourcing Standard* means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. This Outsourcing Standard authorizes access to CHRI for noncriminal justice purposes, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.
- 1.12 *Physically Secure Location* means a facility or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CHRI and associated information systems.
- 1.13 *Positive Identification*, as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints<sup>1</sup> or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other non-unique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.
- 1.14 *Public Carrier Network* means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: Dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.
- 1.15 *Security Violation* means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in

---

<sup>1</sup> The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning positive identification may be obtained from the FBI Compact Council office.

violation of: (A) Federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

2.0 *Responsibilities of the Authorized Recipient*

- 2.01 Prior to engaging in outsourcing any noncriminal justice administrative functions, the Authorized Recipient shall: (a) Request and receive written permission from (1) the State Compact Officer/Chief Administrator<sup>2</sup> or (2) the FBI Compact Officer<sup>3</sup>; (b) provide the Compact Officer/Chief Administrator copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested; and (c) inquire of the FBI Compact Officer whether a prospective Contractor has any security violations (See Section 8.04). The FBI Compact Officer will report those findings to the Authorized Recipient and, when applicable, to the State Compact Officer/Chief Administrator.
- 2.02 The Authorized Recipient shall execute a contract or agreement prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.
- 2.03 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; limit retention of the information to a period of time not to exceed that period of time the Authorized Recipient is permitted to retain such information; prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General; ensure the security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; and ensure that Contractor

---

<sup>2</sup>The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and Authorized Recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.

<sup>3</sup>State or local Authorized Recipients based on State or Federal Statutes shall contact the State Compact Officer/Chief Administrator. Federal or Regulatory Agency Authorized Recipients shall contact the FBI Compact Officer.

personnel comply with this Outsourcing Standard.

- a. The Authorized Recipient shall conduct criminal history record checks of Contractor personnel having access to CHRI if such checks are required or authorized of the Authorized Recipient's personnel having similar access.<sup>4</sup> The Authorized Recipient shall maintain updated records of Contractor personnel who have access to CHRI and update those records within 24 hours when changes to that access occur and, if a criminal history record check is required, the Authorized Recipient shall maintain a list of Contractor personnel who successfully completed the criminal history record check.
  - b. The Authorized Recipient shall ensure that the Contractor maintains site security.
  - c. The Authorized Recipient shall ensure that the most current version of both the Outsourcing Standard and the CJIS Security Policy are incorporated by reference at the time of contract, contract renewal, or within 30 calendar days (unless otherwise directed) of notification of successor versions of the Outsourcing Standard and/or CJIS Security Policy, whichever is sooner. The Authorized Recipient shall notify the Contractor within 30 calendar days (unless otherwise directed) of FBI notification regarding changes or updates to the Outsourcing Standard and/or CJIS Security Policy.
- 2.04 The Authorized Recipient shall understand the communications and record capabilities of the Contractor which has access to federal or state records through, or because of, its outsourcing relationship with the Authorized Recipient. The Authorized Recipient shall maintain an updated topological drawing which depicts the interconnectivity of the Contractor's network configuration.
- 2.05 The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the Outsourcing Standard. The Authorized Recipient shall certify to the Compact Officer/Chief Administrator that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.

---

<sup>4</sup>If a national criminal history record check of Authorized Recipient personnel having access to CHRI is mandated or authorized by a federal statute, executive order, or state statute approved by the Attorney General under Public Law 92-544, the State Compact Officer/Chief Administrator and/or the FBI Compact Officer must ensure Contractor personnel having similar access are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives. The national criminal history record checks of Contractor personnel with access to CHRI cannot be outsourced and must be performed by the Authorized Recipient.

2.06 The Authorized Recipient shall provide written notice of any early voluntary termination of the contract to the Compact Officer/Chief Administrator or the FBI Compact Officer.

3.0 *Responsibilities of the Contractor*

3.01 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the CJIS Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

3.02 The Contractor shall develop, document, administer, and maintain a Security Program (Physical, Personnel, and Information Technology) to comply with the most current Outsourcing Standard and the most current FBI *CJIS Security Policy*. The Security Program shall describe the implementation of the security requirements described in this Outsourcing Standard and the FBI *CJIS Security Policy*. In addition, the Contractor is also responsible to set, maintain, and enforce the standards for the selection, supervision, and separation of personnel who have access to CHRI. The Authorized Recipient shall provide the written approval of a Contractor's Security Program.

3.03 The requirements for a Security Program should include, at a minimum:

- a) Description of the implementation of the security requirements described in this Outsourcing Standard and the *CJIS Security Policy*.
- b) Security Training.
- c) Guidelines for documentation of security violations.
- d) Standards for the selection, supervision, and separation of personnel with access to CHRI.

\*\*If the Contractor is using a corporate policy, it must meet the requirements outlined in this Outsourcing Standard and the *CJIS Security Policy*. If the corporate policy is not this specific, it must flow down to a level where the documentation supports these requirements.

3.04 Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. The Authorized Recipient shall review and provide to the Contractor written approval of the Security Training Program. Training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall annually, not later than the anniversary date of the contract, certify in writing to the Authorized Recipient that annual refresher training was completed for those Contractor personnel with access

to CHRI.

- 3.05 The Contractor shall make its facilities available for announced and unannounced audits performed by the Authorized Recipient, the state, or the FBI on behalf of the Compact Council.
- 3.06 The Contractor's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI CJIS Division. During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.
- 3.07 The Contractor shall maintain CHRI only for the period of time necessary to fulfill its contractual obligations but not to exceed the period of time that the Authorized Recipient is authorized to maintain and does maintain the CHRI.
- 3.08 The Contractor shall maintain a log of any dissemination of CHRI, for a minimum of 365 days.

#### 4.0 *Site Security*

- 4.01 The Authorized Recipient shall ensure that the Contractor site(s) is a physically secure location to protect against any unauthorized access to CHRI.

#### 5.0 *Dissemination*

- 5.01 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 5.02 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) The Authorized Recipient and the secondary recipient with unique identifiers, (B) the record disseminated, (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.
- 5.03 If CHRI is stored or disseminated in an electronic format, the Contractor shall protect against unauthorized access to the equipment and any of the data. In no event shall responses containing CHRI be disseminated other than as governed by this Outsourcing Standard or more stringent contract requirements.

#### 6.0 *Personnel Security*

- 6.01 If a local, state, or federal written standard requires or authorizes a criminal history record check of the Authorized Recipient's personnel with access to

CHRI, then a criminal history record check shall be required of the Contractor's (and approved Sub-Contractor's) employees having access to CHRI. Criminal history record checks of Contractor and approved Sub-Contractor employees, at a minimum, will be no less stringent than criminal history record checks that are performed on the Authorized Recipient's personnel performing similar functions. Criminal history record checks must be completed prior to accessing CHRI under the contract.

- 6.02 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm in writing that each employee has certified in writing that he/she understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities. The Contractor shall maintain the employee certifications in a file that is subject to review during audits. Employees shall make such certification prior to performing work under the contract.
- 6.03 The Contractor shall maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur, and if a criminal history record check is required, maintain a list of personnel who have successfully completed criminal history record checks. The Contractor shall notify Authorized Recipients within 24 hours when additions or deletions occur.

## 7.0 *System Security*

- 7.01 The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy.
  - a. If CHRI can be accessed by unauthorized personnel via Wide Area Network/Local Area Network or the Internet, then the Contractor shall protect the CHRI with firewall-type devices to prevent such unauthorized access. These devices shall implement a minimum firewall profile as specified by the CJIS Security Policy in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.
  - b. Data encryption shall be required throughout the network passing CHRI through a shared public carrier network.
- 7.02 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.
  - a. CHRI shall be stored in a physically secure location.
  - b. The Authorized Recipient shall ensure that a procedure is in place for

sanitizing all fixed storage media (e.g., disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal, or reuse. Sanitization procedures include overwriting the media and/or degaussing the media.

- c. The Authorized Recipient shall ensure that a procedure is in place for the disposal or return of all non-fixed storage media (e.g., hard copies, print-outs).

7.03 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient, Contractor, or sub-Contractor must be assigned a unique identifying number.

## 8.0 *Security Violations*

### 8.01 Duties of the Authorized Recipient and Contractor

- a. The Contractor shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference.
- b. Pending investigation, the Contractor shall, upon detection or awareness, suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.
- c. The Contractor shall immediately (within four hours) notify the Authorized Recipient of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. Within five calendar days of such notification, the Contractor shall provide the Authorized Recipient a written report documenting such security violation, any corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.
- d. The Authorized Recipient shall immediately (within four hours) notify the State Compact Officer/Chief Administrator and the FBI Compact Officer of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator, if applicable, and the FBI Compact Officer, within five calendar days of receipt of the written report from the Contractor. The written report must include any corrective actions taken by the Contractor and the Authorized Recipient to resolve such security violation.



- 8.02 Termination of the contract by the Authorized Recipient for security violations
- a. The contract is subject to termination by the Authorized Recipient for security violations involving CHRI obtained pursuant to the contract.
  - b. The contract is subject to termination by the Authorized Recipient for the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.
  - c. If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient shall terminate the contract.
- 8.03 Suspension or termination of the exchange of CHRI for security violations
- a. Notwithstanding the actions taken by the State Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Compact Council or the United States Attorney General may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 CFR §906.2(d).
  - b. If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United States Attorney General by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be deleted or returned in accordance with the provisions and time frame as specified by the Authorized Recipient.
- 8.04 The Authorized Recipient shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following:
- a. The termination of a contract for security violations.
  - b. Security violations involving the unauthorized access to CHRI.
  - c. The Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.
- 8.05 The Compact Officer/Chief Administrator, Compact Council and the United States Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.
- 8.06 The Compact Officer/Chief Administrator, Compact Council, and the United

States Attorney General reserve the right to audit the Authorized Recipient and the Contractor's operations and procedures at scheduled or unscheduled times. The Compact Council, the United States Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the contract.

#### 9.0 *Miscellaneous Provisions*

- 9.01 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, Compact Officer/Chief Administrator (where applicable), and the FBI.
- 9.02 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) The CJIS Security Policy.
- 9.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and the CHRI accessed therefrom and it is understood that there may be terms and conditions of the appended contract which impose more stringent requirements upon the Contractor.<sup>5</sup>
- 9.04 The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. Conformance to such security measures may not be less stringent than stated in this Outsourcing Standard without the consent of the Compact Council in consultation with the United States Attorney General.
- 9.05 This Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.
- 9.06 Appropriate notices, assurances, and correspondence to the FBI Compact Officer, Compact Council, and the United States Attorney General required by Section 8.0 of this Outsourcing Standard shall be forwarded by First Class Mail to:
  - FBI Compact Officer
  - 1000 Custer Hollow Road
  - Module D-3
  - Clarksburg, WV 26306

#### 10.0 *Exemption from Above Provisions*

---

<sup>5</sup>Such conditions could include additional audits, fees, or security requirements. The Compact Council, Authorized Recipients, and the Compact Officer/Chief Administrator have the explicit authority to require more stringent standards than those contained in the Outsourcing Standard.

- 10.01 An Information Technology (IT) contract need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:
1. Access to CHRI by the IT contractor's personnel is limited solely for the development and/or maintenance of the Authorized Recipient's computer system;
  2. Access to CHRI is incidental, but necessary, to the duties being performed by the IT contractor;
  3. The computer system resides within the Authorized Recipient's facility;
  4. The Authorized Recipient's personnel supervise or work directly with the IT contractor personnel;
  5. The Authorized Recipient maintains complete, positive control of the IT contractor's access to the computer system and CHRI contained therein; and
  6. The Authorized Recipient retains all of the duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard.

10.02 An Authorized Recipient's contract where access to CHRI is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 4.0, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:

1. Access to CHRI by the Contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient;
2. Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor;

3. The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the Authorized Recipient;
4. The Contractor's personnel are subject to the same criminal history record checks as the Authorized Recipient's personnel;
5. The criminal history record checks of the Contractor personnel are completed prior to work on the contract or agreement;
6. The Authorized Recipient retains all other duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard; and
7. The Contractor stores the CHRI in a physically secure location.

WSP Contract No. C130731GSC  
Amendment 1

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above referenced Contract between the Washington State Patrol and the Pasco Police Department is hereby amended as follows:

- The end date shall be extended through September 17, 2021.
- EXHIBIT B CJIS Security Policy 5.1 shall be replaced with EXHIBIT B CJIS Security Policy 5.5.

All other terms and conditions of this Contract remain in full force and effect.

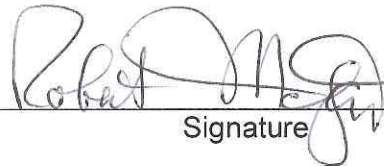
THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

PASCO POLICE DEPARTMENT



FOR: John R. Batiste, Chief



Signature

1-5-17

Date

12-29-16

Date

**MEMORANDUM OF UNDERSTANDING**

**Between the**

**WASHINGTON STATE PATROL**

**And the**

**SPOKANE COUNTY JUVENILE COURT**

**I. PURPOSE**

The parties to this Memorandum of Understanding (MOU) are the Washington State Patrol, Identification and Criminal History Section (WSP) and the Spokane County Juvenile Court, a non criminal justice agency (NCJA). This MOU sets forth the policy to ensure the protection of criminal history record information (CHRI) between the WSP, the NCJA, and the Federal Bureau of Investigation (FBI). This MOU provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CHRI data. This policy applies to the NCJA and its contractors with access to, or who operate in support of, non-criminal justice services and information.

**II. ADMINISTRATIVE RESPONSIBILITIES**

As participants in this MOU, the parties will develop mutually and separately appropriate procedures for transmission, dissemination, storage, and destruction of CHRI data.

a. The Washington State Patrol. WSP shall ensure the NCJA complies with the Criminal Justice Information Services (CJIS) Security Policy (See Exhibit B) which includes authorized use of CHRI, dissemination of CHRI, statute authorization for civil applicant background checks conducted by noncriminal justice agencies, applicant notification and record challenge, security of CHRI, storage of CHRI, outsourcing of noncriminal justice administrative functions, and user fees. WSP will conduct regional audits of all agencies working under this MOU to ensure compliance to all state and federal standards.

b. NCJA. The NCJA shall be responsible for ensuring:

1. NCJA responds to requests for information by the FBI CJIS Division or the WSP in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of the agency.
2. NCJA has formalized written procedures for the following, if applicable: criminal history use and dissemination, misuse, background checks, password management, storage, and destruction of CHRI.
3. CHRI received as a result of licensing or employment purposes, pursuant to Public Law 92-544 is solely used for the purpose for which the record was requested. Subject fingerprints shall be submitted with all requests for CHRI for noncriminal justice purposes. Access to the FBI CJIS using name-based inquiry and record request messages is not permitted for noncriminal justice purpose, unless otherwise approved by the FBI.
4. Access to CHRI by authorized officials is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or other authorized entities.

5. All fingerprint based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.
6. NCJA must notify the applicants fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The officials making the determination of suitability for licensing or employment shall provide the applicants the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record. These officials also must advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in Title 28, C.F.R. 16.34. Official making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so.
7. Appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity.
8. NCJA shall seek WSP permission prior to outsourcing noncriminal justice functions.
9. Outsourcing of noncriminal justice administrative functions requiring access to CHRI to either another governmental agency or a private contractor acting as an agent for the authorized receiving agency complies with the security and management control outsourcing standard for non-channelers (see Exhibit A).
10. NCJA is responsible for compliance to technical standards set forth by WSP and the CJIS Security Policy.
11. NCJA will conduct periodic self audits to ensure compliance with CJIS Security Policy.
12. NCJA will participate in WSP and FBI audits, provide plans for any compliance issues, and follow through to resolution within identified timeframes.
13. NCJA will ensure all appropriate staff members are trained according to the state and federal requirements.

### **III. CRIMINAL HISTORY RECORD INFORMATION RESPONSIBILITIES**

NCJA shall conform to system policies, as established by the FBI CJIS Division and WSP, before access to CHRI is permitted. This will allow for control over the data and give assurance of system security.

1. The rules and procedures governing access to CHRI shall apply equally to all participants in the system.
2. All noncriminal justice agencies with access to CHRI data must designate a specific unit, position, or personnel to access CHRI; noncriminal justice agencies must advise WSP of such personnel and changes to such designation.
3. All noncriminal justice agencies with access to CHRI data from the system shall permit an FBI CJIS Division or WSP audit team to conduct appropriate audits. NCJA must cooperate with these audits and respond promptly.

### **IV. SECURITY RESPONSIBILITIES**

#### **Technical Roles and Responsibilities**

NCJA must comply with and enforce system security. NCJA must have someone designated as the security point of contact (POC). Security POC's shall be responsible for the following:

1. Identifying the user of the hardware/software and ensuring that no unauthorized users have access to the same.
2. Identifying and documenting how the equipment is connected to the state system.

3. Ensuring that personnel security screening procedures are being followed as stated in the CJIS Security Policy.
4. Ensuring that appropriate hardware security measures are in place.
5. Supporting policy compliance and keeping the WSP informed of security incidents.
6. If the technical POC changes at your agency, notify WSP immediately.

#### **Security Enforcement**

NCJA is responsible for enforcing system security standards for their agency, in addition to all of the other agencies to which the NCJA provides CHRI information. Authorized users shall access and disseminate the CHRI data only for the purpose for which they are authorized. NCJA shall have a written policy for the discipline of policy violators.

#### **Technical Security Training**

All Information Technology (IT) employees who have access to and those who have direct responsibility to configure and maintain FBI CJIS systems must review security awareness training within six months of their appointment or assignment. Documentation pertaining to the materials used and those employees which receive security awareness training shall be maintained in a current status.

#### **Physical Security**

A physically secured location in a noncriminal justice facility, an area, a room, a group of rooms, that is/are subject to criminal justice agency management control security addendum and which contain hardware, software, and/or firmware (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch panels, etc.) that provide access to the CJIS sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that restrict unauthorized access.

All personnel with access to computer centers, CHRI, or areas where CHRI information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check. All personnel must review security awareness training within six months of their appointment or assignment.

#### **Personnel Security**

To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days of initial employment or assignment for all personnel who have authorized access to FBI CJIS information and those who have direct responsibility to configure and maintain computer systems and networks with access to FBI CJIS information. All requests from system access shall be made as specified by the CJIS Systems Officer (i.e. WSP Identification and Criminal History Section).

- c. NCJA shall use the data supplied by WSP and the FBI under this MOU only for the authorized purpose intended. NCJA shall not use this data for any other purpose and shall not disseminate this data with any other parties unless required by law. NCJA shall share any public disclosure requests regarding this data with the WSP.

#### **Storage**

Please see 'Security and Management Control Outsourcing Standard for Non-Channelers' (Exhibit A).



**V. LIAISON REPRESENTATIVES**

**For the Washington State Patrol:**

Jim Anderson, Administrator  
Criminal Records Division  
PO Box 42619  
Olympia WA 98504-2619  
Phone: (360) 534-2101  
Fax: (360) 534-2070  
E-mail: [jim.anderson@wsp.wa.gov](mailto:jim.anderson@wsp.wa.gov)

**For the Spokane County Juvenile Court:**

Bonnie Bush  
1208 W Mallon  
Spokane WA 99201  
509-477-2406  
[bbush@spokanecounty.org](mailto:bbush@spokanecounty.org)

**VI. INDEMNIFICATION**

Each party shall defend, protect and hold harmless the other party from and against all claims, suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing this MOU.

**VII. PERIOD OF MOU**

This MOU becomes effective on the date of the last signature and continues for three years and may be renewed. It may be modified by mutual written consent of the two agencies. Liaison Representatives may modify Exhibit A by mutual written consent of the two agencies without changing the general conditions of this MOU.

**VIII. TERMINATION**

Except as otherwise provided in this MOU, either party may terminate this MOU upon ninety (90) days' written notification to the other party. If this MOU is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this MOU for performance prior to the effective date of termination.

**IX. DISPUTES**

In the event that a dispute arises under this MOU, it shall be determined in the following manner: The Chief of WSP, or designee, shall appoint one member to the Dispute Board. NCJA shall appoint one member to the Dispute Board. The Chief of WSP, or designee, and the NCJA shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. If applicable and as an alternative to this process, either of the parties may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.

**X. EXHIBITS**

The exhibits listed below are incorporated into and made a part of this MOU:

Exhibit A - 'Security and Management Control Outsourcing Standard for Non-Channelers'

Exhibit B - Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.2, published 8/9/2013 which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

**XI. ORDER OF PRECEDENCE**

In the event of any inconsistency in the terms of this MOU, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

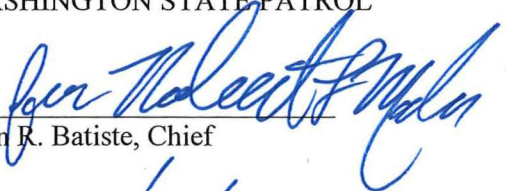
- a. Applicable federal and state statutes and regulations;
- b. The Terms and Conditions contained in this MOU;
- c. The Exhibits attached to this MOU;
- d. Any other provisions of the MOU, whether incorporated by reference or otherwise.

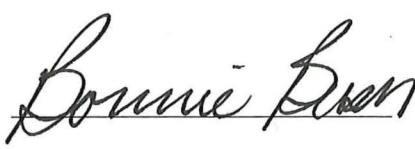
**XII. ALL WRITINGS CONTAINED HEREIN**

This MOU contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this MOU shall be deemed to exist or to bind any of the parties hereto.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

SPOKANE COUNTY JUVENILE COURT

  
\_\_\_\_\_  
John R. Batiste, Chief

  
\_\_\_\_\_  
Bonnie Brown

  
\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Date

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above referenced Contract between the Washington State Patrol and the Spokane County Juvenile Court is hereby amended as follows:

- The end date shall be extended through September 19, 2021.
- EXHIBIT B CJIS Security Policy 5.1 shall be replaced with EXHIBIT B CJIS Security Policy 5.5.

All other terms and conditions of this Contract remain in full force and effect.

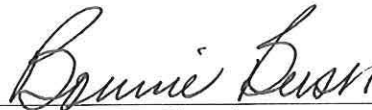
THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

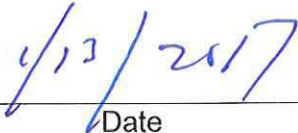
SPOKANE COUNTY  
JUVENILE COURT



FOR: John R. Batiste, Chief



Signature



Date



Date

**MEMORANDUM OF UNDERSTANDING**

**Between the**

**WASHINGTON STATE PATROL**

**And the**

**SKAGIT COUNTY SUPERIOR COURT**

**I. PURPOSE**

The parties to this Memorandum of Understanding (MOU) are the Washington State Patrol, Identification and Criminal History Section (WSP) and the Skagit County Superior Court, a non criminal justice agency (NCJA). This MOU sets forth the policy to ensure the protection of criminal history record information (CHRI) between the WSP, the NCJA, and the Federal Bureau of Investigation (FBI). This MOU provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CHRI data. This policy applies to the NCJA and its contractors with access to, or who operate in support of, non-criminal justice services and information.

**II. ADMINISTRATIVE RESPONSIBILITIES**

As participants in this MOU, the parties will develop mutually and separately appropriate procedures for transmission, dissemination, storage, and destruction of CHRI data.

a. The Washington State Patrol. WSP shall ensure the NCJA complies with the Criminal Justice Information Services (CJIS) Security Policy (See Exhibit B) which includes authorized use of CHRI, dissemination of CHRI, statute authorization for civil applicant background checks conducted by noncriminal justice agencies, applicant notification and record challenge, security of CHRI, storage of CHRI, outsourcing of noncriminal justice administrative functions, and user fees. WSP will conduct regional audits of all agencies working under this MOU to ensure compliance to all state and federal standards.

b. NCJA. The NCJA shall be responsible for ensuring:

1. NCJA responds to requests for information by the FBI CJIS Division or the WSP in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of the agency.
2. NCJA has formalized written procedures for the following, if applicable: criminal history use and dissemination, misuse, background checks, password management, storage, and destruction of CHRI.
3. CHRI received as a result of licensing or employment purposes, pursuant to Public Law 92-544 is solely used for the purpose for which the record was requested. Subject fingerprints shall be submitted with all requests for CHRI for noncriminal justice purposes. Access to the FBI CJIS using name-based inquiry and record request messages is not permitted for noncriminal justice purpose, unless otherwise approved by the FBI.
4. Access to CHRI by authorized officials is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or other authorized entities.

5. All fingerprint based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.
6. NCJA must notify the applicants fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The officials making the determination of suitability for licensing or employment shall provide the applicants the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record. These officials also must advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in Title 28, C.F.R. 16.34. Official making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so.
7. Appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity.
8. NCJA shall seek WSP permission prior to outsourcing noncriminal justice functions.
9. Outsourcing of noncriminal justice administrative functions requiring access to CHRI to either another governmental agency or a private contractor acting as an agent for the authorized receiving agency complies with the security and management control outsourcing standard for non-channelers (see Exhibit A).
10. NCJA is responsible for compliance to technical standards set forth by WSP and the CJIS Security Policy.
11. NCJA will conduct periodic self audits to ensure compliance with CJIS Security Policy.
12. NCJA will participate in WSP and FBI audits, provide plans for any compliance issues, and follow through to resolution within identified timeframes.
13. NCJA will ensure all appropriate staff members are trained according to the state and federal requirements.

### **III. CRIMINAL HISTORY RECORD INFORMATION RESPONSIBILITIES**

NCJA shall conform to system policies, as established by the FBI CJIS Division and WSP, before access to CHRI is permitted. This will allow for control over the data and give assurance of system security.

1. The rules and procedures governing access to CHRI shall apply equally to all participants in the system.
2. ~~All noncriminal justice agencies with access to CHRI data must designate a specific unit, position, or personnel to access CHRI; noncriminal justice agencies must advise WSP of such personnel and changes to such designation.~~
3. All noncriminal justice agencies with access to CHRI data from the system shall permit an FBI CJIS Division or WSP audit team to conduct appropriate audits. NCJA must cooperate with these audits and respond promptly.

### **IV. SECURITY RESPONSIBILITIES**

#### **Technical Roles and Responsibilities**

NCJA must comply with and enforce system security. NCJA must have someone designated as the security point of contact (POC). Security POC's shall be responsible for the following:

1. Identifying the user of the hardware/software and ensuring that no unauthorized users have access to the same.
2. Identifying and documenting how the equipment is connected to the state system.

3. Ensuring that personnel security screening procedures are being followed as stated in the CJIS Security Policy.
4. Ensuring that appropriate hardware security measures are in place.
5. Supporting policy compliance and keeping the WSP informed of security incidents.
6. If the technical POC changes at your agency, notify WSP immediately.

#### **Security Enforcement**

NCJA is responsible for enforcing system security standards for their agency, in addition to all of the other agencies to which the NCJA provides CHRI information. Authorized users shall access and disseminate the CHRI data only for the purpose for which they are authorized. NCJA shall have a written policy for the discipline of policy violators.

#### **Technical Security Training**

All Information Technology (IT) employees who have access to and those who have direct responsibility to configure and maintain FBI CJIS systems must review security awareness training within six months of their appointment or assignment. Documentation pertaining to the materials used and those employees which receive security awareness training shall be maintained in a current status.

#### **Physical Security**

A physically secured location in a noncriminal justice facility, an area, a room, a group of rooms, that is/are subject to criminal justice agency management control security addendum and which contain hardware, software, and/or firmware (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch panels, etc.) that provide access to the CJIS sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that restrict unauthorized access.

All personnel with access to computer centers, CHRI, or areas where CHRI information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check. All personnel must review security awareness training within six months of their appointment or assignment.

#### **Personnel Security**

To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days of initial employment or assignment for all personnel who have authorized access to FBI CJIS information and those who have direct responsibility to configure and maintain computer systems and networks with access to FBI CJIS information. All requests from system access shall be made as specified by the CJIS Systems Officer (i.e. WSP Identification and Criminal History Section).

- c. NCJA shall use the data supplied by WSP and the FBI under this MOU only for the authorized purpose intended. NCJA shall not use this data for any other purpose and shall not disseminate this data with any other parties unless required by law. NCJA shall share any public disclosure requests regarding this data with the WSP.

#### **Storage**

Please see 'Security and Management Control Outsourcing Standard for Non-Channelers' (Exhibit A).

**V. LIAISON REPRESENTATIVES**

**For the Washington State Patrol:**

Jim Anderson, Administrator  
Criminal Records Division  
PO Box 42619  
Olympia WA 98504-2619  
Phone: (360) 534-2101  
Fax:(360) 534-2070  
E-mail: [jim.anderson@wsp.wa.gov](mailto:jim.anderson@wsp.wa.gov)

**For the Skagit County Superior Court:**

Delilah M. George  
205 W Kincaid St Rm 202  
Mount Vernon WA 98273  
360-336-9325  
[delilahg@co.skagit.wa.us](mailto:delilahg@co.skagit.wa.us)

**VI. INDEMNIFICATION**

Each party shall defend, protect and hold harmless the other party from and against all claims, suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing this MOU.

**VII. PERIOD OF MOU**

This MOU becomes effective on the date of the last signature and continues for three years and may be renewed. It may be modified by mutual written consent of the two agencies. Liaison Representatives may modify Exhibit A by mutual written consent of the two agencies without changing the general conditions of this MOU.

**VIII. TERMINATION**

Except as otherwise provided in this MOU, either party may terminate this MOU upon ninety (90) days' written notification to the other party. If this MOU is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this MOU for performance prior to the effective date of termination.

**IX. DISPUTES**

In the event that a dispute arises under this MOU, it shall be determined in the following manner: The Chief of WSP, or designee, shall appoint one member to the Dispute Board. NCJA shall appoint one member to the Dispute Board. The Chief of WSP, or designee, and the NCJA shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. If applicable and as an alternative to this process, either of the parties may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.

**X. EXHIBITS**

The exhibits listed below are incorporated into and made a part of this MOU:

Exhibit A - 'Security and Management Control Outsourcing Standard for Non-Channelers'

Exhibit B - Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version ~~5.2~~<sup>5.3</sup> published ~~8/9/2013~~<sup>8/4/2014</sup> which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

**XI. ORDER OF PRECEDENCE**

In the event of any inconsistency in the terms of this MOU, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:


- a. Applicable federal and state statutes and regulations;
- b. The Terms and Conditions contained in this MOU;
- c. The Exhibits attached to this MOU;
- d. Any other provisions of the MOU, whether incorporated by reference or otherwise.

**XII. ALL WRITINGS CONTAINED HEREIN**

This MOU contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this MOU shall be deemed to exist or to bind any of the parties hereto.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

SKAGIT COUNTY SUPERIOR COURT

*for*   
\_\_\_\_\_  
John R. Batiste, Chief

*see attached*  
\_\_\_\_\_

*02/10/19*  
\_\_\_\_\_  
Date

\_\_\_\_\_  
Date



DATED this 29 day of September, 2014.

BOARD OF COUNTY COMMISSIONERS  
SKAGIT COUNTY, WASHINGTON



Ron Wesen, Chair



Kenneth A. Dahlstedt, Commissioner



Sharon D. Dillon, Commissioner

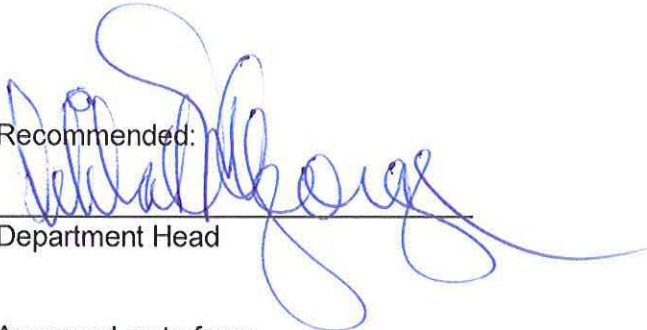
Attest:



Clerk of the Board

For contracts under \$5,000:  
Authorization per Resolution R20030146

Recommended:



Department Head

\_\_\_\_\_  
County Administrator

Approved as to form:



Civil Deputy Prosecuting Attorney

Approved as to indemnification:



Risk Manager

Approved as to budget:



Budget & Finance Director

## SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD for NON-CHANNELERS

The goal of this document is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the Contractor. Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security and Management Control Outsourcing Standard (Outsourcing Standard) is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI without a direct connection to the FBI CJIS Wide Area Network (WAN).

### 1.0 Definitions

- 1.01 *Access to CHRI* means to view or make use of CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by title 42, United States Code, section 14614(b).
- 1.02 *Authorized Recipient* means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.
- 1.03 *Chief Administrator* means the primary administrator of a Nonparty State’s criminal history record repository or a designee of such administrator who is

a regular full-time employee of the repository, which is also referred to as the State Identification Bureau (SIB) Chief.

- 1.04 *CHRI*, as referred to in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.
- 1.05 *Criminal History Record Check*, for purposes of this Outsourcing Standard only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.
- 1.06 *Compact Officer*, as provided in Article I(2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the compact among federal agencies], or (B) with respect to a Party State, the chief administrator of the State's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.
- 1.07 *Contractor* means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI.
- 1.08 *Dissemination* means the disclosure of CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 1.09 *Noncriminal Justice Administrative Functions* means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:
1. Making fitness determinations/recommendations
  2. Obtaining missing dispositions
  3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General
  4. Other authorized activities relating to the general handling, use, and storage of CHRI

- 1.10 *Noncriminal Justice Purposes*, as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.
- 1.11 *Outsourcing Standard* means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. This Outsourcing Standard authorizes access to CHRI for noncriminal justice purposes, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.
- 1.12 *Physically Secure Location* means a facility or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CHRI and associated information systems.
- 1.13 *Positive Identification*, as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints<sup>1</sup> or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other non-unique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.
- 1.14 *Public Carrier Network* means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: Dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.
- 1.15 *Security Violation* means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in

---

<sup>1</sup> The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning positive identification may be obtained from the FBI Compact Council office.

violation of: (A) Federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

2.0 *Responsibilities of the Authorized Recipient*

- 2.01 Prior to engaging in outsourcing any noncriminal justice administrative functions, the Authorized Recipient shall: (a) Request and receive written permission from (1) the State Compact Officer/Chief Administrator<sup>2</sup> or (2) the FBI Compact Officer<sup>3</sup>; (b) provide the Compact Officer/Chief Administrator copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested; and (c) inquire of the FBI Compact Officer whether a prospective Contractor has any security violations (See Section 8.04). The FBI Compact Officer will report those findings to the Authorized Recipient and, when applicable, to the State Compact Officer/Chief Administrator.
- 2.02 The Authorized Recipient shall execute a contract or agreement prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.
- 2.03 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; limit retention of the information to a period of time not to exceed that period of time the Authorized Recipient is permitted to retain such information; prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General; ensure the security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; and ensure that Contractor

---

<sup>2</sup>The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and Authorized Recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.

<sup>3</sup>State or local Authorized Recipients based on State or Federal Statutes shall contact the State Compact Officer/Chief Administrator. Federal or Regulatory Agency Authorized Recipients shall contact the FBI Compact Officer.

personnel comply with this Outsourcing Standard.

- a. The Authorized Recipient shall conduct criminal history record checks of Contractor personnel having access to CHRI if such checks are required or authorized of the Authorized Recipient's personnel having similar access.<sup>4</sup> The Authorized Recipient shall maintain updated records of Contractor personnel who have access to CHRI and update those records within 24 hours when changes to that access occur and, if a criminal history record check is required, the Authorized Recipient shall maintain a list of Contractor personnel who successfully completed the criminal history record check.
  - b. The Authorized Recipient shall ensure that the Contractor maintains site security.
  - c. The Authorized Recipient shall ensure that the most current version of both the Outsourcing Standard and the CJIS Security Policy are incorporated by reference at the time of contract, contract renewal, or within 30 calendar days (unless otherwise directed) of notification of successor versions of the Outsourcing Standard and/or CJIS Security Policy, whichever is sooner. The Authorized Recipient shall notify the Contractor within 30 calendar days (unless otherwise directed) of FBI notification regarding changes or updates to the Outsourcing Standard and/or CJIS Security Policy.
- 2.04 The Authorized Recipient shall understand the communications and record capabilities of the Contractor which has access to federal or state records through, or because of, its outsourcing relationship with the Authorized Recipient. The Authorized Recipient shall maintain an updated topological drawing which depicts the interconnectivity of the Contractor's network configuration.
- 2.05 The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the Outsourcing Standard. The Authorized Recipient shall certify to the Compact Officer/Chief Administrator that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.

---

<sup>4</sup>If a national criminal history record check of Authorized Recipient personnel having access to CHRI is mandated or authorized by a federal statute, executive order, or state statute approved by the Attorney General under Public Law 92-544, the State Compact Officer/Chief Administrator and/or the FBI Compact Officer must ensure Contractor personnel having similar access are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives. The national criminal history record checks of Contractor personnel with access to CHRI cannot be outsourced and must be performed by the Authorized Recipient.

- 2.06 The Authorized Recipient shall provide written notice of any early voluntary termination of the contract to the Compact Officer/Chief Administrator or the FBI Compact Officer.

3.0 *Responsibilities of the Contractor*

- 3.01 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the CJIS Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 3.02 The Contractor shall develop, document, administer, and maintain a Security Program (Physical, Personnel, and Information Technology) to comply with the most current Outsourcing Standard and the most current FBI *CJIS Security Policy*. The Security Program shall describe the implementation of the security requirements described in this Outsourcing Standard and the FBI *CJIS Security Policy*. In addition, the Contractor is also responsible to set, maintain, and enforce the standards for the selection, supervision, and separation of personnel who have access to CHRI. The Authorized Recipient shall provide the written approval of a Contractor's Security Program.
- 3.03 The requirements for a Security Program should include, at a minimum:
- a) Description of the implementation of the security requirements described in this Outsourcing Standard and the *CJIS Security Policy*.
  - b) Security Training.
  - c) Guidelines for documentation of security violations.
  - d) Standards for the selection, supervision, and separation of personnel with access to CHRI.

\*\*If the Contractor is using a corporate policy, it must meet the requirements outlined in this Outsourcing Standard and the *CJIS Security Policy*. If the corporate policy is not this specific, it must flow down to a level where the documentation supports these requirements.

- 3.04 Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. The Authorized Recipient shall review and provide to the Contractor written approval of the Security Training Program. Training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall annually, not later than the anniversary date of the contract, certify in writing to the Authorized Recipient that annual refresher training was completed for those Contractor personnel with access

- to CHRI.
- 3.05 The Contractor shall make its facilities available for announced and unannounced audits performed by the Authorized Recipient, the state, or the FBI on behalf of the Compact Council.
  - 3.06 The Contractor's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI CJIS Division. During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.
  - 3.07 The Contractor shall maintain CHRI only for the period of time necessary to fulfill its contractual obligations but not to exceed the period of time that the Authorized Recipient is authorized to maintain and does maintain the CHRI.
  - 3.08 The Contractor shall maintain a log of any dissemination of CHRI, for a minimum of 365 days.
- 4.0 *Site Security*
- 4.01 The Authorized Recipient shall ensure that the Contractor site(s) is a physically secure location to protect against any unauthorized access to CHRI.
- 5.0 *Dissemination*
- 5.01 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.
  - 5.02 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) The Authorized Recipient and the secondary recipient with unique identifiers, (B) the record disseminated, (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.
  - 5.03 If CHRI is stored or disseminated in an electronic format, the Contractor shall protect against unauthorized access to the equipment and any of the data. In no event shall responses containing CHRI be disseminated other than as governed by this Outsourcing Standard or more stringent contract requirements.
- 6.0 *Personnel Security*
- 6.01 If a local, state, or federal written standard requires or authorizes a criminal history record check of the Authorized Recipient's personnel with access to



CHRI, then a criminal history record check shall be required of the Contractor's (and approved Sub-Contractor's) employees having access to CHRI. Criminal history record checks of Contractor and approved Sub-Contractor employees, at a minimum, will be no less stringent than criminal history record checks that are performed on the Authorized Recipient's personnel performing similar functions. Criminal history record checks must be completed prior to accessing CHRI under the contract.

- 6.02 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm in writing that each employee has certified in writing that he/she understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities. The Contractor shall maintain the employee certifications in a file that is subject to review during audits. Employees shall make such certification prior to performing work under the contract.
- 6.03 The Contractor shall maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur, and if a criminal history record check is required, maintain a list of personnel who have successfully completed criminal history record checks. The Contractor shall notify Authorized Recipients within 24 hours when additions or deletions occur.

## 7.0 *System Security*

- 7.01 The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy.
  - a. If CHRI can be accessed by unauthorized personnel via Wide Area Network/Local Area Network or the Internet, then the Contractor shall protect the CHRI with firewall-type devices to prevent such unauthorized access. These devices shall implement a minimum firewall profile as specified by the CJIS Security Policy in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.
  - b. Data encryption shall be required throughout the network passing CHRI through a shared public carrier network.
- 7.02 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.
  - a. CHRI shall be stored in a physically secure location.
  - b. The Authorized Recipient shall ensure that a procedure is in place for

sanitizing all fixed storage media (e.g., disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal, or reuse. Sanitization procedures include overwriting the media and/or degaussing the media.

- c. The Authorized Recipient shall ensure that a procedure is in place for the disposal or return of all non-fixed storage media (e.g., hard copies, print-outs).
- 7.03 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient, Contractor, or sub-Contractor must be assigned a unique identifying number.

## 8.0 *Security Violations*

### 8.01 Duties of the Authorized Recipient and Contractor

- a. The Contractor shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference.
- b. Pending investigation, the Contractor shall, upon detection or awareness, suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.
- c. The Contractor shall immediately (within four hours) notify the Authorized Recipient of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. Within five calendar days of such notification, the Contractor shall provide the Authorized Recipient a written report documenting such security violation, any corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.
- d. The Authorized Recipient shall immediately (within four hours) notify the State Compact Officer/Chief Administrator and the FBI Compact Officer of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator, if applicable, and the FBI Compact Officer, within five calendar days of receipt of the written report from the Contractor. The written report must include any corrective actions taken by the Contractor and the Authorized Recipient to resolve such security violation.

- 8.02 Termination of the contract by the Authorized Recipient for security violations
- a. The contract is subject to termination by the Authorized Recipient for security violations involving CHRI obtained pursuant to the contract.
  - b. The contract is subject to termination by the Authorized Recipient for the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.
  - c. If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient shall terminate the contract.
- 8.03 Suspension or termination of the exchange of CHRI for security violations
- a. Notwithstanding the actions taken by the State Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Compact Council or the United States Attorney General may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 CFR §906.2(d).
  - b. If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United States Attorney General by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be deleted or returned in accordance with the provisions and time frame as specified by the Authorized Recipient.
- 
- 8.04 The Authorized Recipient shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following:
- a. The termination of a contract for security violations.
  - b. Security violations involving the unauthorized access to CHRI.
  - c. The Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.
- 8.05 The Compact Officer/Chief Administrator, Compact Council and the United States Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.
- 8.06 The Compact Officer/Chief Administrator, Compact Council, and the United

States Attorney General reserve the right to audit the Authorized Recipient and the Contractor's operations and procedures at scheduled or unscheduled times. The Compact Council, the United States Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the contract.

9.0 *Miscellaneous Provisions*

- 9.01 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, Compact Officer/Chief Administrator (where applicable), and the FBI.
- 9.02 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) The CJIS Security Policy.
- 9.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and the CHRI accessed therefrom and it is understood that there may be terms and conditions of the appended contract which impose more stringent requirements upon the Contractor.<sup>5</sup>
- 9.04 The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. Conformance to such security measures may not be less stringent than stated in this Outsourcing Standard without the consent of the Compact Council in consultation with the United States Attorney General.
- 9.05 This Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.
- 9.06 Appropriate notices, assurances, and correspondence to the FBI Compact Officer, Compact Council, and the United States Attorney General required by Section 8.0 of this Outsourcing Standard shall be forwarded by First Class Mail to:

FBI Compact Officer  
1000 Custer Hollow Road  
Module D-3  
Clarksburg, WV 26306

10.0 *Exemption from Above Provisions*

---

<sup>5</sup>Such conditions could include additional audits, fees, or security requirements. The Compact Council, Authorized Recipients, and the Compact Officer/Chief Administrator have the explicit authority to require more stringent standards than those contained in the Outsourcing Standard.

- 10.01 An Information Technology (IT) contract need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:
1. Access to CHRI by the IT contractor's personnel is limited solely for the development and/or maintenance of the Authorized Recipient's computer system;
  2. Access to CHRI is incidental, but necessary, to the duties being performed by the IT contractor;
  3. The computer system resides within the Authorized Recipient's facility;
  4. The Authorized Recipient's personnel supervise or work directly with the IT contractor personnel;
  5. The Authorized Recipient maintains complete, positive control of the IT contractor's access to the computer system and CHRI contained therein; and
  6. The Authorized Recipient retains all of the duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard.

10.02 An Authorized Recipient's contract where access to CHRI is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 4.0, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:

1. Access to CHRI by the Contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient;
2. Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor;

3. The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the Authorized Recipient;
4. The Contractor's personnel are subject to the same criminal history record checks as the Authorized Recipient's personnel;
5. The criminal history record checks of the Contractor personnel are completed prior to work on the contract or agreement;
6. The Authorized Recipient retains all other duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard; and
7. The Contractor stores the CHRI in a physically secure location.

---

BILL REQUEST - CODE REVISER'S OFFICE

---

BILL REQ. #: Z-0453.2/13 2nd draft

ATTY/TYPIST: AI:eab

BRIEF DESCRIPTION: Concerning noncriminal history records checks.

1 AN ACT Relating to noncriminal history records checks; amending RCW  
2 43.43.700, 43.43.705, and 43.43.742; and repealing RCW 28A.400.306.

3 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

4 **Sec. 1.** RCW 43.43.700 and 2006 c 294 s 1 are each amended to read  
5 as follows:

6 (1) There is hereby established within the Washington state patrol  
7 a section on identification and criminal history hereafter referred to  
8 as the section.

9 (2) In order to aid the administration of justice the section shall  
10 install systems for the identification of individuals, including the  
11 fingerprint system and such other systems as the chief deems necessary.  
12 The section shall keep a complete record and index of all information  
13 received in convenient form for consultation and comparison.

14 (3) The section shall obtain from whatever source available and  
15 file for record the fingerprints, palmprints, photographs, or such  
16 other identification data as it deems necessary, of persons who have  
17 been or shall hereafter be lawfully arrested and charged with, or  
18 convicted of any criminal offense. The section may obtain like



1 information concerning persons arrested for or convicted of crimes  
2 under the laws of another state or government.

3 (4) The section may:

4 (a) Retain the fingerprints submitted by a statutorily authorized  
5 agency or entity;

6 (b) Allow a search by criminal justice agencies of arrest  
7 fingerprint submissions and unsolved crime files against the  
8 fingerprints submitted for noncriminal justice purposes;

9 (c) Notify a statutorily authorized agency or entity of a change in  
10 criminal history record information that is identified against retained  
11 fingerprints. The section must ensure that arrest information is  
12 provided only to a statutorily authorized agency or entity from which  
13 the fingerprints originated.

14 (5) A statutorily authorized agency or entity must notify license  
15 applicants and applicants for employment subject to a criminal history  
16 background check that their fingerprints may be retained by the section  
17 and the federal bureau of investigation. A statutorily authorized  
18 agency or entity must also provide notification to license applicants  
19 and applicants for employment that:

20 (a) Arrests and unsolved crime files may be searched against their  
21 retained fingerprints.

22 (b) Notification of any changes to criminal history record  
23 information may be made to the statutorily authorized agency or entity  
24 that submitted the fingerprints to the section.

25 **Sec. 2.** RCW 43.43.705 and 2006 c 294 s 2 are each amended to read  
26 as follows:

27 Upon the receipt of identification data from criminal justice  
28 agencies within this state, the section shall immediately cause the  
29 files to be examined and upon request shall promptly return to the  
30 contributor of such data a transcript of the record of previous arrests  
31 and dispositions of the persons described in the data submitted.

32 Upon application, the section shall furnish to criminal justice  
33 agencies a transcript of the criminal history record information  
34 available pertaining to any person of whom the section has a record.

35 For the purposes of RCW 43.43.700 through 43.43.785 the following  
36 words and phrases shall have the following meanings:

1 "Criminal history record information" includes, and shall be  
2 restricted to identifying data and information recorded as the result  
3 of an arrest or other initiation of criminal proceedings and the  
4 consequent proceedings related thereto. "Criminal history record  
5 information" shall not include intelligence, analytical, or  
6 investigative reports and files.

7 "Criminal justice agencies" are those public agencies within or  
8 outside the state which perform, as a principal function, activities  
9 directly relating to the apprehension, prosecution, adjudication or  
10 rehabilitation of criminal offenders.

11 "Statutorily authorized agency or entity" means a public agency or  
12 private entity that has statutory authority, under state, federal, or  
13 local law, to conduct a state and federal criminal history background  
14 check for license applicants, applicants for employment, or other  
15 noncriminal justice purposes.

16 The section may refuse to furnish any information pertaining to the  
17 identification or history of any person or persons of whom it has a  
18 record, or other information in its files and records, to any applicant  
19 if the chief determines that the applicant has previously misused  
20 information furnished to such applicant by the section or the chief  
21 believes that the applicant will not use the information requested  
22 solely for the purpose of due administration of the criminal laws or  
23 for the purposes enumerated in RCW 43.43.760(4). The applicant may  
24 appeal such determination by notifying the chief in writing within  
25 thirty days. The hearing shall be before an administrative law judge  
26 appointed under chapter 34.12 RCW and in accordance with procedures for  
27 adjudicative proceedings under chapter 34.05 RCW.

28 **Sec. 3.** RCW 43.43.742 and 1987 c 450 s 4 are each amended to read  
29 as follows:

30 (1) The Washington state patrol shall adopt rules concerning  
31 submission of fingerprints taken by local agencies ((after July 26,  
32 1987,)) from persons for license application or other noncriminal  
33 purposes.

34 (2) The Washington state patrol must adopt rules concerning the  
35 participation of statutorily authorized agencies or other entities in  
36 receiving notifications of any changes to criminal history records

1 information after the submission of fingerprints taken by local  
2 agencies for noncriminal purposes.

3 (3) The Washington state patrol may charge fees for submission of  
4 fingerprints which will cover as nearly as practicable the direct and  
5 indirect costs to the Washington state patrol of processing such  
6 submission or notifying a statutorily authorized agency or entity of a  
7 change in criminal history record information as provided in RCW  
8 43.43.700.

9 NEW SECTION. Sec. 4. RCW 28A.400.306 (Fingerprints accepted by  
10 the state patrol--Fingerprints forwarded to the federal bureau of  
11 investigation--Conditions) and 1995 c 335 s 504 & 1992 c 159 s 9 are  
12 each repealed.

--- END ---

WSP Contract No. C130736GSC  
Amendment 1

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above referenced Contract between the Washington State Patrol and the Skagit County Superior Court is hereby amended as follows:

- The end date shall be extended through October 10, 2022.
- **Exhibit B** "CJIS Security Policy" shall be replaced by **Exhibit B** – Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.5, published 6/1/2016 which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.
- The effective date of this Amendment shall be October 10, 2017.

All other terms and conditions of this Contract remain in full force and effect.

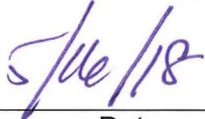
THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

SKAGIT COUNTY SUPERIOR COURT



FOR: John R. Batiste, Chief



Date



Signature



Date

DATED this 26 day of March, 2018.

**BOARD OF COUNTY COMMISSIONERS  
SKAGIT COUNTY, WASHINGTON**

**ABSENT**

\_\_\_\_\_  
Kenneth A. Dahlstedt, Chair

Lisa Janicki

\_\_\_\_\_  
Lisa Janicki, Commissioner

Ron Wesen

\_\_\_\_\_  
Ron Wesen, Commissioner

Attest:

Amber Epps  
\_\_\_\_\_  
Clerk of the Board

For contracts under \$5,000:  
Authorization per Resolution R20030146

Recommended:

Li Tremblay  
\_\_\_\_\_  
Department Head

\_\_\_\_\_  
County Administrator

Approved as to form:

M. Noel 3/21/2018  
\_\_\_\_\_  
Civil Deputy Prosecuting Attorney

Approved as to indemnification:

Shawn O'Bois (3-26-18)  
\_\_\_\_\_  
Risk Manager

Approved as to budget:

Justin Legno  
\_\_\_\_\_  
Budget & Finance Director

**MEMORANDUM OF UNDERSTANDING**

**Between the**

**WASHINGTON STATE PATROL**

**And the**

**YAKIMA COUNTY JUVENILE COURT**

**I. PURPOSE**

The parties to this Memorandum of Understanding (MOU) are the Washington State Patrol, Identification and Criminal History Section (WSP) and the Yakima County Juvenile Court, a non criminal justice agency (NCJA). This MOU sets forth the policy to ensure the protection of criminal history record information (CHRI) between the WSP, the NCJA, and the Federal Bureau of Investigation (FBI). This MOU provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CHRI data. This policy applies to the NCJA and its contractors with access to, or who operate in support of, non-criminal justice services and information.

**II. ADMINISTRATIVE RESPONSIBILITIES**

As participants in this MOU, the parties will develop mutually and separately appropriate procedures for transmission, dissemination, storage, and destruction of CHRI data.

- a. The Washington State Patrol. WSP shall ensure the NCJA complies with the Criminal Justice Information Services (CJIS) Security Policy (See Exhibit B) which includes authorized use of CHRI, dissemination of CHRI, statute authorization for civil applicant background checks conducted by noncriminal justice agencies, applicant notification and record challenge, security of CHRI, storage of CHRI, outsourcing of noncriminal justice administrative functions, and user fees. WSP will conduct regional audits of all agencies working under this MOU to ensure compliance to all state and federal standards.
- b. NCJA. The NCJA shall be responsible for ensuring:
  1. NCJA responds to requests for information by the FBI CJIS Division or the WSP in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of the agency.
  2. NCJA has formalized written procedures for the following, if applicable: criminal history use and dissemination, misuse, background checks, password management, storage, and destruction of CHRI.
  3. CHRI received as a result of licensing or employment purposes, pursuant to Public Law 92-544 is solely used for the purpose for which the record was requested. Subject fingerprints shall be submitted with all requests for CHRI for noncriminal justice purposes. Access to the FBI CJIS using name-based inquiry and record request messages is not permitted for noncriminal justice purpose, unless otherwise approved by the FBI.
  4. Access to CHRI by authorized officials is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or other authorized entities.

5. All fingerprint based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.
6. NCJA must notify the applicants fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The officials making the determination of suitability for licensing or employment shall provide the applicants the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record. These officials also must advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in Title 28, C.F.R. 16.34. Official making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so.
7. Appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity.
8. NCJA shall seek WSP permission prior to outsourcing noncriminal justice functions.
9. Outsourcing of noncriminal justice administrative functions requiring access to CHRI to either another governmental agency or a private contractor acting as an agent for the authorized receiving agency complies with the security and management control outsourcing standard for non-channelers (see Exhibit A).
10. NCJA is responsible for compliance to technical standards set forth by WSP and the CJIS Security Policy.
11. NCJA will conduct periodic self audits to ensure compliance with CJIS Security Policy.
12. NCJA will participate in WSP and FBI audits, provide plans for any compliance issues, and follow through to resolution within identified timeframes.
13. NCJA will ensure all appropriate staff members are trained according to the state and federal requirements.

### **III. CRIMINAL HISTORY RECORD INFORMATION RESPONSIBILITIES**

NCJA shall conform to system policies, as established by the FBI CJIS Division and WSP, before access to CHRI is permitted. This will allow for control over the data and give assurance of system security.

1. The rules and procedures governing access to CHRI shall apply equally to all participants in the system.
2. All noncriminal justice agencies with access to CHRI data must designate a specific unit, position, or personnel to access CHRI; noncriminal justice agencies must advise WSP of such personnel and changes to such designation.
3. All noncriminal justice agencies with access to CHRI data from the system shall permit an FBI CJIS Division or WSP audit team to conduct appropriate audits. NCJA must cooperate with these audits and respond promptly.

### **IV. SECURITY RESPONSIBILITIES**

#### **Technical Roles and Responsibilities**

NCJA must comply with and enforce system security. NCJA must have someone designated as the security point of contact (POC). Security POC's shall be responsible for the following:

1. Identifying the user of the hardware/software and ensuring that no unauthorized users have access to the same.
2. Identifying and documenting how the equipment is connected to the state system.

3. Ensuring that personnel security screening procedures are being followed as stated in the CJIS Security Policy.
4. Ensuring that appropriate hardware security measures are in place.
5. Supporting policy compliance and keeping the WSP informed of security incidents.
6. If the technical POC changes at your agency, notify WSP immediately.

#### **Security Enforcement**

NCJA is responsible for enforcing system security standards for their agency, in addition to all of the other agencies to which the NCJA provides CHRI information. Authorized users shall access and disseminate the CHRI data only for the purpose for which they are authorized. NCJA shall have a written policy for the discipline of policy violators.

#### **Technical Security Training**

All Information Technology (IT) employees who have access to and those who have direct responsibility to configure and maintain FBI CJIS systems must review security awareness training within six months of their appointment or assignment. Documentation pertaining to the materials used and those employees which receive security awareness training shall be maintained in a current status.

#### **Physical Security**

A physically secured location in a noncriminal justice facility, an area, a room, a group of rooms, that is/are subject to criminal justice agency management control security addendum and which contain hardware, software, and/or firmware (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch panels, etc.) that provide access to the CJIS sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that restrict unauthorized access.

All personnel with access to computer centers, CHRI, or areas where CHRI information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check. All personnel must review security awareness training within six months of their appointment or assignment.

#### **Personnel Security**

To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days of initial employment or assignment for all personnel who have authorized access to FBI CJIS information and those who have direct responsibility to configure and maintain computer systems and networks with access to FBI CJIS information. All requests from system access shall be made as specified by the CJIS Systems Officer (i.e. WSP Identification and Criminal History Section).

- c. NCJA shall use the data supplied by WSP and the FBI under this MOU only for the authorized purpose intended. NCJA shall not use this data for any other purpose and shall not disseminate this data with any other parties unless required by law. NCJA shall share any public disclosure requests regarding this data with the WSP.

#### **Storage**

Please see 'Security and Management Control Outsourcing Standard for Non-Channelers' (Exhibit A).



**V. LIAISON REPRESENTATIVES**

**For the Washington State Patrol:**

Jim Anderson, Administrator  
Criminal Records Division  
PO Box 42619  
Olympia WA 98504-2619  
Phone: (360) 534-2101  
Fax: (360) 534-2070  
E-mail: [jim.anderson@wsp.wa.gov](mailto:jim.anderson@wsp.wa.gov)

**For the Yakima County Juvenile Court:**

Frank Murray  
1728 Jerome Ave  
Yakima WA 98902  
509-574-2071  
[frank.murray@co.yakima.wa.us](mailto:frank.murray@co.yakima.wa.us)

**VI. INDEMNIFICATION**

Each party shall defend, protect and hold harmless the other party from and against all claims, suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing this MOU.

**VII. PERIOD OF MOU**

This MOU becomes effective on the date of the last signature and continues for three years and may be renewed. It may be modified by mutual written consent of the two agencies. Liaison Representatives may modify Exhibit A by mutual written consent of the two agencies without changing the general conditions of this MOU.

**VIII. TERMINATION**

Except as otherwise provided in this MOU, either party may terminate this MOU upon ninety (90) days' written notification to the other party. If this MOU is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this MOU for performance prior to the effective date of termination.

**IX. DISPUTES**

In the event that a dispute arises under this MOU, it shall be determined in the following manner: The Chief of WSP, or designee, shall appoint one member to the Dispute Board. NCJA shall appoint one member to the Dispute Board. The Chief of WSP, or designee, and the NCJA shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. If applicable and as an alternative to this process, either of the parties may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.

**X. EXHIBITS**

The exhibits listed below are incorporated into and made a part of this MOU:

Exhibit A - 'Security and Management Control Outsourcing Standard for Non-Channelers'

Exhibit B - Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.2, published 8/9/2013 which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

**XI. ORDER OF PRECEDENCE**

In the event of any inconsistency in the terms of this MOU, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

- a. Applicable federal and state statutes and regulations;
- b. The Terms and Conditions contained in this MOU;
- c. The Exhibits attached to this MOU;
- d. Any other provisions of the MOU, whether incorporated by reference or otherwise.

**XII. ALL WRITINGS CONTAINED HEREIN**

This MOU contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this MOU shall be deemed to exist or to bind any of the parties hereto.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

YAKIMA COUNTY JUVENILE COURT

*for Simon Lee*  
\_\_\_\_\_  
John R. Batiste, Chief

*Robyn Berndt*  
\_\_\_\_\_

*10-14-13*  
\_\_\_\_\_  
Date

*9/17/13*  
\_\_\_\_\_  
Date

## SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD for NON-CHANNELERS

The goal of this document is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the Contractor. Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security and Management Control Outsourcing Standard (Outsourcing Standard) is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI without a direct connection to the FBI CJIS Wide Area Network (WAN).

### 1.0 *Definitions*

- 1.01 *Access to CHRI* means to view or make use of CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by title 42, United States Code, section 14614(b).
- 1.02 *Authorized Recipient* means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.
- 1.03 *Chief Administrator* means the primary administrator of a Nonparty State’s criminal history record repository or a designee of such administrator who is

a regular full-time employee of the repository, which is also referred to as the State Identification Bureau (SIB) Chief.

- 1.04 *CHRI*, as referred to in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.
- 1.05 *Criminal History Record Check*, for purposes of this Outsourcing Standard only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.
- 1.06 *Compact Officer*, as provided in Article I(2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the compact among federal agencies], or (B) with respect to a Party State, the chief administrator of the State's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.
- 1.07 *Contractor* means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI.
- 1.08 *Dissemination* means the disclosure of CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 1.09 *Noncriminal Justice Administrative Functions* means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:
1. Making fitness determinations/recommendations
  2. Obtaining missing dispositions
  3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General
  4. Other authorized activities relating to the general handling, use, and storage of CHRI

- 1.10 *Noncriminal Justice Purposes*, as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.
- 1.11 *Outsourcing Standard* means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. This Outsourcing Standard authorizes access to CHRI for noncriminal justice purposes, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.
- 1.12 *Physically Secure Location* means a facility or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CHRI and associated information systems.
- 1.13 *Positive Identification*, as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints<sup>1</sup> or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other non-unique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.
- 1.14 *Public Carrier Network* means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: Dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.
- 1.15 *Security Violation* means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in

---

<sup>1</sup> The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning positive identification may be obtained from the FBI Compact Council office.

violation of: (A) Federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

*2.0 Responsibilities of the Authorized Recipient*

- 2.01 Prior to engaging in outsourcing any noncriminal justice administrative functions, the Authorized Recipient shall: (a) Request and receive written permission from (1) the State Compact Officer/Chief Administrator<sup>2</sup> or (2) the FBI Compact Officer<sup>3</sup>; (b) provide the Compact Officer/Chief Administrator copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested; and (c) inquire of the FBI Compact Officer whether a prospective Contractor has any security violations (See Section 8.04). The FBI Compact Officer will report those findings to the Authorized Recipient and, when applicable, to the State Compact Officer/Chief Administrator.
- 2.02 The Authorized Recipient shall execute a contract or agreement prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.
- 2.03 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; limit retention of the information to a period of time not to exceed that period of time the Authorized Recipient is permitted to retain such information; prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General; ensure the security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; and ensure that Contractor

---

<sup>2</sup>The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and Authorized Recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.

<sup>3</sup>State or local Authorized Recipients based on State or Federal Statutes shall contact the State Compact Officer/Chief Administrator. Federal or Regulatory Agency Authorized Recipients shall contact the FBI Compact Officer.

personnel comply with this Outsourcing Standard.

- a. The Authorized Recipient shall conduct criminal history record checks of Contractor personnel having access to CHRI if such checks are required or authorized of the Authorized Recipient's personnel having similar access.<sup>4</sup> The Authorized Recipient shall maintain updated records of Contractor personnel who have access to CHRI and update those records within 24 hours when changes to that access occur and, if a criminal history record check is required, the Authorized Recipient shall maintain a list of Contractor personnel who successfully completed the criminal history record check.
  - b. The Authorized Recipient shall ensure that the Contractor maintains site security.
  - c. The Authorized Recipient shall ensure that the most current version of both the Outsourcing Standard and the CJIS Security Policy are incorporated by reference at the time of contract, contract renewal, or within 30 calendar days (unless otherwise directed) of notification of successor versions of the Outsourcing Standard and/or CJIS Security Policy, whichever is sooner. The Authorized Recipient shall notify the Contractor within 30 calendar days (unless otherwise directed) of FBI notification regarding changes or updates to the Outsourcing Standard and/or CJIS Security Policy.
- 2.04 The Authorized Recipient shall understand the communications and record capabilities of the Contractor which has access to federal or state records through, or because of, its outsourcing relationship with the Authorized Recipient. The Authorized Recipient shall maintain an updated topological drawing which depicts the interconnectivity of the Contractor's network configuration.
- 2.05 The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the Outsourcing Standard. The Authorized Recipient shall certify to the Compact Officer/Chief Administrator that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.

---

<sup>4</sup>If a national criminal history record check of Authorized Recipient personnel having access to CHRI is mandated or authorized by a federal statute, executive order, or state statute approved by the Attorney General under Public Law 92-544, the State Compact Officer/Chief Administrator and/or the FBI Compact Officer must ensure Contractor personnel having similar access are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives. The national criminal history record checks of Contractor personnel with access to CHRI cannot be outsourced and must be performed by the Authorized Recipient.

2.06 The Authorized Recipient shall provide written notice of any early voluntary termination of the contract to the Compact Officer/Chief Administrator or the FBI Compact Officer.

3.0 *Responsibilities of the Contractor*

3.01 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the CJIS Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

3.02 The Contractor shall develop, document, administer, and maintain a Security Program (Physical, Personnel, and Information Technology) to comply with the most current Outsourcing Standard and the most current FBI *CJIS Security Policy*. The Security Program shall describe the implementation of the security requirements described in this Outsourcing Standard and the FBI *CJIS Security Policy*. In addition, the Contractor is also responsible to set, maintain, and enforce the standards for the selection, supervision, and separation of personnel who have access to CHRI. The Authorized Recipient shall provide the written approval of a Contractor's Security Program.

3.03 The requirements for a Security Program should include, at a minimum:

- a) Description of the implementation of the security requirements described in this Outsourcing Standard and the *CJIS Security Policy*.
- b) Security Training.
- c) Guidelines for documentation of security violations.
- d) Standards for the selection, supervision, and separation of personnel with access to CHRI.

\*\*If the Contractor is using a corporate policy, it must meet the requirements outlined in this Outsourcing Standard and the *CJIS Security Policy*. If the corporate policy is not this specific, it must flow down to a level where the documentation supports these requirements.

3.04 Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. The Authorized Recipient shall review and provide to the Contractor written approval of the Security Training Program. Training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall annually, not later than the anniversary date of the contract, certify in writing to the Authorized Recipient that annual refresher training was completed for those Contractor personnel with access



to CHRI.

- 3.05 The Contractor shall make its facilities available for announced and unannounced audits performed by the Authorized Recipient, the state, or the FBI on behalf of the Compact Council.
- 3.06 The Contractor's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI CJIS Division. During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.
- 3.07 The Contractor shall maintain CHRI only for the period of time necessary to fulfill its contractual obligations but not to exceed the period of time that the Authorized Recipient is authorized to maintain and does maintain the CHRI.
- 3.08 The Contractor shall maintain a log of any dissemination of CHRI, for a minimum of 365 days.

#### 4.0 *Site Security*

- 4.01 The Authorized Recipient shall ensure that the Contractor site(s) is a physically secure location to protect against any unauthorized access to CHRI.

#### 5.0 *Dissemination*

- 5.01 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 5.02 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) The Authorized Recipient and the secondary recipient with unique identifiers, (B) the record disseminated, (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.
- 5.03 If CHRI is stored or disseminated in an electronic format, the Contractor shall protect against unauthorized access to the equipment and any of the data. In no event shall responses containing CHRI be disseminated other than as governed by this Outsourcing Standard or more stringent contract requirements.

#### 6.0 *Personnel Security*

- 6.01 If a local, state, or federal written standard requires or authorizes a criminal history record check of the Authorized Recipient's personnel with access to

CHRI, then a criminal history record check shall be required of the Contractor's (and approved Sub-Contractor's) employees having access to CHRI. Criminal history record checks of Contractor and approved Sub-Contractor employees, at a minimum, will be no less stringent than criminal history record checks that are performed on the Authorized Recipient's personnel performing similar functions. Criminal history record checks must be completed prior to accessing CHRI under the contract.

- 6.02 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm in writing that each employee has certified in writing that he/she understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities. The Contractor shall maintain the employee certifications in a file that is subject to review during audits. Employees shall make such certification prior to performing work under the contract.
- 6.03 The Contractor shall maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur, and if a criminal history record check is required, maintain a list of personnel who have successfully completed criminal history record checks. The Contractor shall notify Authorized Recipients within 24 hours when additions or deletions occur.

## 7.0 *System Security*

- 7.01 The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy.
  - a. If CHRI can be accessed by unauthorized personnel via Wide Area Network/Local Area Network or the Internet, then the Contractor shall protect the CHRI with firewall-type devices to prevent such unauthorized access. These devices shall implement a minimum firewall profile as specified by the CJIS Security Policy in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.
  - b. Data encryption shall be required throughout the network passing CHRI through a shared public carrier network.
- 7.02 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.
  - a. CHRI shall be stored in a physically secure location.
  - b. The Authorized Recipient shall ensure that a procedure is in place for

sanitizing all fixed storage media (e.g., disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal, or reuse. Sanitization procedures include overwriting the media and/or degaussing the media.

- c. The Authorized Recipient shall ensure that a procedure is in place for the disposal or return of all non-fixed storage media (e.g., hard copies, print-outs).

7.03 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient, Contractor, or sub-Contractor must be assigned a unique identifying number.

## 8.0 *Security Violations*

### 8.01 Duties of the Authorized Recipient and Contractor

- a. The Contractor shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference.
- b. Pending investigation, the Contractor shall, upon detection or awareness, suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.
- c. The Contractor shall immediately (within four hours) notify the Authorized Recipient of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. Within five calendar days of such notification, the Contractor shall provide the Authorized Recipient a written report documenting such security violation, any corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.
- d. The Authorized Recipient shall immediately (within four hours) notify the State Compact Officer/Chief Administrator and the FBI Compact Officer of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator, if applicable, and the FBI Compact Officer, within five calendar days of receipt of the written report from the Contractor. The written report must include any corrective actions taken by the Contractor and the Authorized Recipient to resolve such security violation.

- 8.02 Termination of the contract by the Authorized Recipient for security violations
- a. The contract is subject to termination by the Authorized Recipient for security violations involving CHRI obtained pursuant to the contract.
  - b. The contract is subject to termination by the Authorized Recipient for the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.
  - c. If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient shall terminate the contract.
- 8.03 Suspension or termination of the exchange of CHRI for security violations
- a. Notwithstanding the actions taken by the State Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Compact Council or the United States Attorney General may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 CFR §906.2(d).
  - b. If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United States Attorney General by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be deleted or returned in accordance with the provisions and time frame as specified by the Authorized Recipient.
- 8.04 The Authorized Recipient shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following:
- a. The termination of a contract for security violations.
  - b. Security violations involving the unauthorized access to CHRI.
  - c. The Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.
- 8.05 The Compact Officer/Chief Administrator, Compact Council and the United States Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.
- 8.06 The Compact Officer/Chief Administrator, Compact Council, and the United

States Attorney General reserve the right to audit the Authorized Recipient and the Contractor's operations and procedures at scheduled or unscheduled times. The Compact Council, the United States Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the contract.

#### 9.0 *Miscellaneous Provisions*

- 9.01 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, Compact Officer/Chief Administrator (where applicable), and the FBI.
- 9.02 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) The CJIS Security Policy.
- 9.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and the CHRI accessed therefrom and it is understood that there may be terms and conditions of the appended contract which impose more stringent requirements upon the Contractor.<sup>5</sup>
- 9.04 The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. Conformance to such security measures may not be less stringent than stated in this Outsourcing Standard without the consent of the Compact Council in consultation with the United States Attorney General.
- 9.05 This Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.
- 9.06 Appropriate notices, assurances, and correspondence to the FBI Compact Officer, Compact Council, and the United States Attorney General required by Section 8.0 of this Outsourcing Standard shall be forwarded by First Class Mail to:
  - FBI Compact Officer
  - 1000 Custer Hollow Road
  - Module D-3
  - Clarksburg, WV 26306

#### 10.0 *Exemption from Above Provisions*

---

<sup>5</sup>Such conditions could include additional audits, fees, or security requirements. The Compact Council, Authorized Recipients, and the Compact Officer/Chief Administrator have the explicit authority to require more stringent standards than those contained in the Outsourcing Standard.

- 10.01 An Information Technology (IT) contract need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:
1. Access to CHRI by the IT contractor's personnel is limited solely for the development and/or maintenance of the Authorized Recipient's computer system;
  2. Access to CHRI is incidental, but necessary, to the duties being performed by the IT contractor;
  3. The computer system resides within the Authorized Recipient's facility;
  4. The Authorized Recipient's personnel supervise or work directly with the IT contractor personnel;
  5. The Authorized Recipient maintains complete, positive control of the IT contractor's access to the computer system and CHRI contained therein; and
  6. The Authorized Recipient retains all of the duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard.

- 10.02 An Authorized Recipient's contract where access to CHRI is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 4.0, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:
1. Access to CHRI by the Contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient;
  2. Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor;

3. The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the Authorized Recipient;
4. The Contractor's personnel are subject to the same criminal history record checks as the Authorized Recipient's personnel;
5. The criminal history record checks of the Contractor personnel are completed prior to work on the contract or agreement;
6. The Authorized Recipient retains all other duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard; and
7. The Contractor stores the CHRI in a physically secure location.

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above referenced Contract between the Washington State Patrol and the Yakima County Juvenile Court is hereby amended as follows:

- The end date shall be extended through June 30, 2022.
- **Exhibit B** "CJIS Security Policy" shall be replaced by **Exhibit B** – Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.6, published 6/5/2017 which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.
- Section V – Liaison Representatives for the Yakima County Juvenile Court:  
Frank Murray  
1728 Jerome Ave  
Yakima WA 98902  
509-574-2071  
[Frank.murray@co.yakima.wa.us](mailto:Frank.murray@co.yakima.wa.us)


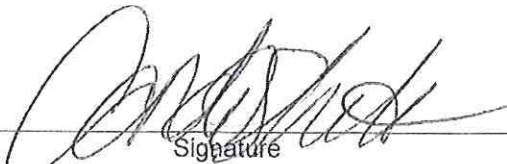
Shall be replaced by:  
Keith Gilberston, Administrative Supervisor for C.A.S.A.  
1728 Jerome Ave  
Yakima WA 98902  
509-574-2071  
[keith.gilberston@co.yakima.wa.us](mailto:keith.gilberston@co.yakima.wa.us)

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

YAKIMA COUNTY JUVENILE COURT

  
\_\_\_\_\_  
FOR: John R. Batiste, Chief  
\_\_\_\_\_  
Signature

9/8/17  
\_\_\_\_\_  
Date

9/5/17  
\_\_\_\_\_  
Date



**MEMORANDUM OF UNDERSTANDING**

**Between the**

**WASHINGTON STATE PATROL**

**And the**

**BREMERTON HOUSING AUTHORITY**

**I. PURPOSE**

The parties to this Memorandum of Understanding (MOU) are the Washington State Patrol, Identification and Criminal History Section (WSP) and the Bremerton Housing Authority, a non criminal justice agency (NCJA). This MOU sets forth the policy to ensure the protection of criminal history record information (CHRI) between the WSP, the NCJA, and the Federal Bureau of Investigation (FBI). This MOU provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CHRI data. This policy applies to the NCJA and its contractors with access to, or who operate in support of, non-criminal justice services and information.

**II. ADMINISTRATIVE RESPONSIBILITIES**

As participants in this MOU, the parties will develop mutually and separately appropriate procedures for transmission, dissemination, storage, and destruction of CHRI data.

- a. The Washington State Patrol. WSP shall ensure the NCJA complies with the Criminal Justice Information Services (CJIS) Security Policy (See Exhibit B) which includes authorized use of CHRI, dissemination of CHRI, statute authorization for civil applicant background checks conducted by noncriminal justice agencies, applicant notification and record challenge, security of CHRI, storage of CHRI, outsourcing of noncriminal justice administrative functions, and user fees. WSP will conduct regional audits of all agencies working under this MOU to ensure compliance to all state and federal standards.
- b. NCJA. The NCJA shall be responsible for ensuring:
  1. NCJA responds to requests for information by the FBI CJIS Division or the WSP in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of the agency.
  2. NCJA has formalized written procedures for the following, if applicable: criminal history use and dissemination, misuse, background checks, password management, storage, and destruction of CHRI.
  3. CHRI received as a result of licensing or employment purposes, pursuant to Public Law 92-544 is solely used for the purpose for which the record was requested. Subject fingerprints shall be submitted with all requests for CHRI for noncriminal justice purposes. Access to the FBI CJIS using name-based inquiry and record request messages is not permitted for noncriminal justice purpose, unless otherwise approved by the FBI.
  4. Access to CHRI by authorized officials is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or other authorized entities.

5. All fingerprint based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.
6. NCJA must notify the applicants fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The officials making the determination of suitability for licensing or employment shall provide the applicants the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record. These officials also must advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in Title 28, C.F.R. 16.34. Official making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so.
7. Appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity.
8. NCJA shall seek WSP permission prior to outsourcing noncriminal justice functions.
9. Outsourcing of noncriminal justice administrative functions requiring access to CHRI to either another governmental agency or a private contractor acting as an agent for the authorized receiving agency complies with the security and management control outsourcing standard for non-channelers (see Exhibit A).
10. NCJA is responsible for compliance to technical standards set forth by WSP and the CJIS Security Policy.
11. NCJA will conduct periodic self audits to ensure compliance with CJIS Security Policy.
12. NCJA will participate in WSP and FBI audits, provide plans for any compliance issues, and follow through to resolution within identified timeframes.
13. NCJA will ensure all appropriate staff members are trained according to the state and federal requirements.

### **III. CRIMINAL HISTORY RECORD INFORMATION RESPONSIBILITIES**

NCJA shall conform to system policies, as established by the FBI CJIS Division and WSP, before access to CHRI is permitted. This will allow for control over the data and give assurance of system security.

1. The rules and procedures governing access to CHRI shall apply equally to all participants in the system.
2. All noncriminal justice agencies with access to CHRI data must designate a specific unit, position, or personnel to access CHRI; noncriminal justice agencies must advise WSP of such personnel and changes to such designation.
3. All noncriminal justice agencies with access to CHRI data from the system shall permit an FBI CJIS Division or WSP audit team to conduct appropriate audits. NCJA must cooperate with these audits and respond promptly.

### **IV. SECURITY RESPONSIBILITIES**

#### **Technical Roles and Responsibilities**

NCJA must comply with and enforce system security. NCJA must have someone designated as the security point of contact (POC). Security POC's shall be responsible for the following:

1. Identifying the user of the hardware/software and ensuring that no unauthorized users have access to the same.
2. Identifying and documenting how the equipment is connected to the state system.

3. Ensuring that personnel security screening procedures are being followed as stated in the CJIS Security Policy.
4. Ensuring that appropriate hardware security measures are in place.
5. Supporting policy compliance and keeping the WSP informed of security incidents.
6. If the technical POC changes at your agency, notify WSP immediately.

### **Security Enforcement**

NCJA is responsible for enforcing system security standards for their agency, in addition to all of the other agencies to which the NCJA provides CHRI information. Authorized users shall access and disseminate the CHRI data only for the purpose for which they are authorized. NCJA shall have a written policy for the discipline of policy violators.

### **Technical Security Training**

All Information Technology (IT) employees who have access to and those who have direct responsibility to configure and maintain FBI CJIS systems must review security awareness training within six months of their appointment or assignment. Documentation pertaining to the materials used and those employees which receive security awareness training shall be maintained in a current status.

### **Physical Security**

A physically secured location in a noncriminal justice facility, an area, a room, a group of rooms, that is/are subject to criminal justice agency management control security addendum and which contain hardware, software, and/or firmware (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch panels, etc.) that provide access to the CJIS sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that restrict unauthorized access.

All personnel with access to computer centers, CHRI, or areas where CHRI information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check. All personnel must review security awareness training within six months of their appointment or assignment.

### **Personnel Security**

To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days of initial employment or assignment for all personnel who have authorized access to FBI CJIS information and those who have direct responsibility to configure and maintain computer systems and networks with access to FBI CJIS information. All requests from system access shall be made as specified by the CJIS Systems Officer (i.e. WSP Identification and Criminal History Section).

- c. NCJA shall use the data supplied by WSP and the FBI under this MOU only for the authorized purpose intended. NCJA shall not use this data for any other purpose and shall not disseminate this data with any other parties unless required by law. NCJA shall share any public disclosure requests regarding this data with the WSP.

### **Storage**

Please see 'Security and Management Control Outsourcing Standard for Non-Channelers' (Exhibit A).

**V. LIAISON REPRESENTATIVES**

**For the Washington State Patrol:**

Jim Anderson, Administrator  
Criminal Records Division  
PO Box 42619  
Olympia WA 98504-2619  
Phone: (360) 534-2101  
Fax: (360) 534-2070  
E-mail: [jim.anderson@wsp.wa.gov](mailto:jim.anderson@wsp.wa.gov)

**For the Bremerton Housing Authority:**

Janine Stevens  
PO Box 2189  
Bremerton WA 98310  
360-616-7125  
[jstevens@bremertonhousing.org](mailto:jstevens@bremertonhousing.org)

**VI. INDEMNIFICATION**

Each party shall defend, protect and hold harmless the other party from and against all claims, suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing this MOU.

**VII. PERIOD OF MOU**

This MOU becomes effective on the date of the last signature and continues for three years and may be renewed. It may be modified by mutual written consent of the two agencies. Liaison Representatives may modify Exhibit A by mutual written consent of the two agencies without changing the general conditions of this MOU.

**VIII. TERMINATION**

Except as otherwise provided in this MOU, either party may terminate this MOU upon ninety (90) days' written notification to the other party. If this MOU is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this MOU for performance prior to the effective date of termination.

**IX. DISPUTES**

In the event that a dispute arises under this MOU, it shall be determined in the following manner: The Chief of WSP, or designee, shall appoint one member to the Dispute Board. NCJA shall appoint one member to the Dispute Board. The Chief of WSP, or designee, and the NCJA shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. If applicable and as an alternative to this process, either of the parties may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.

**X. EXHIBITS**

The exhibits listed below are incorporated into and made a part of this MOU:

Exhibit A - 'Security and Management Control Outsourcing Standard for Non-Channelers'

Exhibit B - Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.2, published 8/9/2013 which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

**XI. ORDER OF PRECEDENCE**

In the event of any inconsistency in the terms of this MOU, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

- a. Applicable federal and state statutes and regulations;
- b. The Terms and Conditions contained in this MOU;
- c. The Exhibits attached to this MOU;
- d. Any other provisions of the MOU, whether incorporated by reference or otherwise.

**XII. ALL WRITINGS CONTAINED HEREIN**

This MOU contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this MOU shall be deemed to exist or to bind any of the parties hereto.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

BREMERTON HOUSING AUTHORITY

  
\_\_\_\_\_  
John R. Batiste, Chief

\_\_\_\_\_  
Date

9/27/13

  
\_\_\_\_\_

\_\_\_\_\_  
Date

9.24.2013

## SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD for NON-CHANNELERS

The goal of this document is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the Contractor. Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security and Management Control Outsourcing Standard (Outsourcing Standard) is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI without a direct connection to the FBI CJIS Wide Area Network (WAN).

### 1.0 *Definitions*

- 1.01 *Access to CHRI* means to view or make use of CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by title 42, United States Code, section 14614(b).
- 1.02 *Authorized Recipient* means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.
- 1.03 *Chief Administrator* means the primary administrator of a Nonparty State’s criminal history record repository or a designee of such administrator who is

a regular full-time employee of the repository, which is also referred to as the State Identification Bureau (SIB) Chief.

- 1.04 *CHRI*, as referred to in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.
- 1.05 *Criminal History Record Check*, for purposes of this Outsourcing Standard only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.
- 1.06 *Compact Officer*, as provided in Article I(2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the compact among federal agencies], or (B) with respect to a Party State, the chief administrator of the State's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.
- 1.07 *Contractor* means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI.
- 1.08 *Dissemination* means the disclosure of CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 1.09 *Noncriminal Justice Administrative Functions* means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:
1. Making fitness determinations/recommendations
  2. Obtaining missing dispositions
  3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General
  4. Other authorized activities relating to the general handling, use, and storage of CHRI

- 1.10 *Noncriminal Justice Purposes*, as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.
- 1.11 *Outsourcing Standard* means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. This Outsourcing Standard authorizes access to CHRI for noncriminal justice purposes, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.
- 1.12 *Physically Secure Location* means a facility or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CHRI and associated information systems.
- 1.13 *Positive Identification*, as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints<sup>1</sup> or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other non-unique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.
- 1.14 *Public Carrier Network* means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: Dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.
- 1.15 *Security Violation* means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in

---

<sup>1</sup> The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning positive identification may be obtained from the FBI Compact Council office.



violation of: (A) Federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

2.0 *Responsibilities of the Authorized Recipient*

- 2.01 Prior to engaging in outsourcing any noncriminal justice administrative functions, the Authorized Recipient shall: (a) Request and receive written permission from (1) the State Compact Officer/Chief Administrator<sup>2</sup> or (2) the FBI Compact Officer<sup>3</sup>; (b) provide the Compact Officer/Chief Administrator copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested; and (c) inquire of the FBI Compact Officer whether a prospective Contractor has any security violations (See Section 8.04). The FBI Compact Officer will report those findings to the Authorized Recipient and, when applicable, to the State Compact Officer/Chief Administrator.
- 2.02 The Authorized Recipient shall execute a contract or agreement prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.
- 2.03 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; limit retention of the information to a period of time not to exceed that period of time the Authorized Recipient is permitted to retain such information; prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General; ensure the security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; and ensure that Contractor

---

<sup>2</sup>The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and Authorized Recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.

<sup>3</sup>State or local Authorized Recipients based on State or Federal Statutes shall contact the State Compact Officer/Chief Administrator. Federal or Regulatory Agency Authorized Recipients shall contact the FBI Compact Officer.

personnel comply with this Outsourcing Standard.

- a. The Authorized Recipient shall conduct criminal history record checks of Contractor personnel having access to CHRI if such checks are required or authorized of the Authorized Recipient's personnel having similar access.<sup>4</sup> The Authorized Recipient shall maintain updated records of Contractor personnel who have access to CHRI and update those records within 24 hours when changes to that access occur and, if a criminal history record check is required, the Authorized Recipient shall maintain a list of Contractor personnel who successfully completed the criminal history record check.
  - b. The Authorized Recipient shall ensure that the Contractor maintains site security.
  - c. The Authorized Recipient shall ensure that the most current version of both the Outsourcing Standard and the CJIS Security Policy are incorporated by reference at the time of contract, contract renewal, or within 30 calendar days (unless otherwise directed) of notification of successor versions of the Outsourcing Standard and/or CJIS Security Policy, whichever is sooner. The Authorized Recipient shall notify the Contractor within 30 calendar days (unless otherwise directed) of FBI notification regarding changes or updates to the Outsourcing Standard and/or CJIS Security Policy.
- 2.04 The Authorized Recipient shall understand the communications and record capabilities of the Contractor which has access to federal or state records through, or because of, its outsourcing relationship with the Authorized Recipient. The Authorized Recipient shall maintain an updated topological drawing which depicts the interconnectivity of the Contractor's network configuration.
- 2.05 The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the Outsourcing Standard. The Authorized Recipient shall certify to the Compact Officer/Chief Administrator that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.

---

<sup>4</sup>If a national criminal history record check of Authorized Recipient personnel having access to CHRI is mandated or authorized by a federal statute, executive order, or state statute approved by the Attorney General under Public Law 92-544, the State Compact Officer/Chief Administrator and/or the FBI Compact Officer must ensure Contractor personnel having similar access are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives. The national criminal history record checks of Contractor personnel with access to CHRI cannot be outsourced and must be performed by the Authorized Recipient.

2.06 The Authorized Recipient shall provide written notice of any early voluntary termination of the contract to the Compact Officer/Chief Administrator or the FBI Compact Officer.

3.0 *Responsibilities of the Contractor*

3.01 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the CJIS Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

3.02 The Contractor shall develop, document, administer, and maintain a Security Program (Physical, Personnel, and Information Technology) to comply with the most current Outsourcing Standard and the most current FBI *CJIS Security Policy*. The Security Program shall describe the implementation of the security requirements described in this Outsourcing Standard and the FBI *CJIS Security Policy*. In addition, the Contractor is also responsible to set, maintain, and enforce the standards for the selection, supervision, and separation of personnel who have access to CHRI. The Authorized Recipient shall provide the written approval of a Contractor's Security Program.

3.03 The requirements for a Security Program should include, at a minimum:

- a) Description of the implementation of the security requirements described in this Outsourcing Standard and the *CJIS Security Policy*.
- b) Security Training.
- c) Guidelines for documentation of security violations.
- d) Standards for the selection, supervision, and separation of personnel with access to CHRI.

*\*\*If the Contractor is using a corporate policy, it must meet the requirements outlined in this Outsourcing Standard and the *CJIS Security Policy*. If the corporate policy is not this specific, it must flow down to a level where the documentation supports these requirements.*

3.04 Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. The Authorized Recipient shall review and provide to the Contractor written approval of the Security Training Program. Training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall annually, not later than the anniversary date of the contract, certify in writing to the Authorized Recipient that annual refresher training was completed for those Contractor personnel with access

to CHRI.

- 3.05 The Contractor shall make its facilities available for announced and unannounced audits performed by the Authorized Recipient, the state, or the FBI on behalf of the Compact Council.
- 3.06 The Contractor's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI CJIS Division. During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.
- 3.07 The Contractor shall maintain CHRI only for the period of time necessary to fulfill its contractual obligations but not to exceed the period of time that the Authorized Recipient is authorized to maintain and does maintain the CHRI.
- 3.08 The Contractor shall maintain a log of any dissemination of CHRI, for a minimum of 365 days.

#### 4.0 *Site Security*

- 4.01 The Authorized Recipient shall ensure that the Contractor site(s) is a physically secure location to protect against any unauthorized access to CHRI.

#### 5.0 *Dissemination*

- 5.01 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 5.02 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) The Authorized Recipient and the secondary recipient with unique identifiers, (B) the record disseminated, (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.
- 5.03 If CHRI is stored or disseminated in an electronic format, the Contractor shall protect against unauthorized access to the equipment and any of the data. In no event shall responses containing CHRI be disseminated other than as governed by this Outsourcing Standard or more stringent contract requirements.

#### 6.0 *Personnel Security*

- 6.01 If a local, state, or federal written standard requires or authorizes a criminal history record check of the Authorized Recipient's personnel with access to

CHRI, then a criminal history record check shall be required of the Contractor's (and approved Sub-Contractor's) employees having access to CHRI. Criminal history record checks of Contractor and approved Sub-Contractor employees, at a minimum, will be no less stringent than criminal history record checks that are performed on the Authorized Recipient's personnel performing similar functions. Criminal history record checks must be completed prior to accessing CHRI under the contract.

- 6.02 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm in writing that each employee has certified in writing that he/she understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities. The Contractor shall maintain the employee certifications in a file that is subject to review during audits. Employees shall make such certification prior to performing work under the contract.
- 6.03 The Contractor shall maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur, and if a criminal history record check is required, maintain a list of personnel who have successfully completed criminal history record checks. The Contractor shall notify Authorized Recipients within 24 hours when additions or deletions occur.

## 7.0 *System Security*

- 7.01 The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy.
  - a. If CHRI can be accessed by unauthorized personnel via Wide Area Network/Local Area Network or the Internet, then the Contractor shall protect the CHRI with firewall-type devices to prevent such unauthorized access. These devices shall implement a minimum firewall profile as specified by the CJIS Security Policy in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.
  - b. Data encryption shall be required throughout the network passing CHRI through a shared public carrier network.
- 7.02 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.
  - a. CHRI shall be stored in a physically secure location.
  - b. The Authorized Recipient shall ensure that a procedure is in place for

sanitizing all fixed storage media (e.g., disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal, or reuse. Sanitization procedures include overwriting the media and/or degaussing the media.

- c. The Authorized Recipient shall ensure that a procedure is in place for the disposal or return of all non-fixed storage media (e.g., hard copies, print-outs).

7.03 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient, Contractor, or sub-Contractor must be assigned a unique identifying number.

## 8.0 *Security Violations*

### 8.01 Duties of the Authorized Recipient and Contractor

- a. The Contractor shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference.
- b. Pending investigation, the Contractor shall, upon detection or awareness, suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.
- c. The Contractor shall immediately (within four hours) notify the Authorized Recipient of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. Within five calendar days of such notification, the Contractor shall provide the Authorized Recipient a written report documenting such security violation, any corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.
- d. The Authorized Recipient shall immediately (within four hours) notify the State Compact Officer/Chief Administrator and the FBI Compact Officer of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator, if applicable, and the FBI Compact Officer, within five calendar days of receipt of the written report from the Contractor. The written report must include any corrective actions taken by the Contractor and the Authorized Recipient to resolve such security violation.

- 8.02 Termination of the contract by the Authorized Recipient for security violations
- a. The contract is subject to termination by the Authorized Recipient for security violations involving CHRI obtained pursuant to the contract.
  - b. The contract is subject to termination by the Authorized Recipient for the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.
  - c. If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient shall terminate the contract.
- 8.03 Suspension or termination of the exchange of CHRI for security violations
- a. Notwithstanding the actions taken by the State Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Compact Council or the United States Attorney General may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 CFR §906.2(d).
  - b. If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United States Attorney General by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be deleted or returned in accordance with the provisions and time frame as specified by the Authorized Recipient.
- 8.04 The Authorized Recipient shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following:
- a. The termination of a contract for security violations.
  - b. Security violations involving the unauthorized access to CHRI.
  - c. The Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.
- 8.05 The Compact Officer/Chief Administrator, Compact Council and the United States Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.
- 8.06 The Compact Officer/Chief Administrator, Compact Council, and the United

States Attorney General reserve the right to audit the Authorized Recipient and the Contractor's operations and procedures at scheduled or unscheduled times. The Compact Council, the United States Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the contract.

#### 9.0 *Miscellaneous Provisions*

- 9.01 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, Compact Officer/Chief Administrator (where applicable), and the FBI.
- 9.02 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) The CJIS Security Policy.
- 9.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and the CHRI accessed therefrom and it is understood that there may be terms and conditions of the appended contract which impose more stringent requirements upon the Contractor.<sup>5</sup>
- 9.04 The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. Conformance to such security measures may not be less stringent than stated in this Outsourcing Standard without the consent of the Compact Council in consultation with the United States Attorney General.
- 9.05 This Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.
- 9.06 Appropriate notices, assurances, and correspondence to the FBI Compact Officer, Compact Council, and the United States Attorney General required by Section 8.0 of this Outsourcing Standard shall be forwarded by First Class Mail to:
  - FBI Compact Officer
  - 1000 Custer Hollow Road
  - Module D-3
  - Clarksburg, WV 26306

#### 10.0 *Exemption from Above Provisions*

---

<sup>5</sup>Such conditions could include additional audits, fees, or security requirements. The Compact Council, Authorized Recipients, and the Compact Officer/Chief Administrator have the explicit authority to require more stringent standards than those contained in the Outsourcing Standard.



- 10.01 An Information Technology (IT) contract need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:
1. Access to CHRI by the IT contractor's personnel is limited solely for the development and/or maintenance of the Authorized Recipient's computer system;
  2. Access to CHRI is incidental, but necessary, to the duties being performed by the IT contractor;
  3. The computer system resides within the Authorized Recipient's facility;
  4. The Authorized Recipient's personnel supervise or work directly with the IT contractor personnel;
  5. The Authorized Recipient maintains complete, positive control of the IT contractor's access to the computer system and CHRI contained therein; and
  6. The Authorized Recipient retains all of the duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard.

10.02 An Authorized Recipient's contract where access to CHRI is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 4.0, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:

1. Access to CHRI by the Contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient;
2. Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor;

3. The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the Authorized Recipient;
4. The Contractor's personnel are subject to the same criminal history record checks as the Authorized Recipient's personnel;
5. The criminal history record checks of the Contractor personnel are completed prior to work on the contract or agreement;
6. The Authorized Recipient retains all other duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard; and
7. The Contractor stores the CHRI in a physically secure location.

WSP Contract No. C130744GSC  
Amendment 1

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above referenced Contract between the Washington State Patrol and the Bremerton Housing Authority is hereby amended as follows:

- The end date shall be extended through September 26, 2021.
- EXHIBIT B CJIS Security Policy 5.1 shall be replaced with EXHIBIT B CJIS Security Policy 5.5.

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

BREMERTON HOUSING AUTHORITY



FOR: John R. Batiste, Chief



Signature

3/2/17  
Date

2/21/2017  
Date

RECEIVED  
MAY 1 2017  
PROPERTY & FINANCE  
WSP

**MEMORANDUM OF UNDERSTANDING**

**Between the**

**WASHINGTON STATE PATROL**

**And the**

**ISLAND COUNTY  
HOUSING AUTHORITY**

**I. PURPOSE**

The parties to this Memorandum of Understanding (MOU) are the Washington State Patrol, Identification and Criminal History Section (WSP) and the Island County Housing Authority, a non criminal justice agency (NCJA). This MOU sets forth the policy to ensure the protection of criminal history record information (CHRI) between the WSP, the NCJA, and the Federal Bureau of Investigation (FBI). This MOU provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CHRI data. This policy applies to the NCJA and its contractors with access to, or who operate in support of, non-criminal justice services and information.

**II. ADMINISTRATIVE RESPONSIBILITIES**

As participants in this MOU, the parties will develop mutually and separately appropriate procedures for transmission, dissemination, storage, and destruction of CHRI data.

- a. The Washington State Patrol. WSP shall ensure the NCJA complies with the Criminal Justice Information Services (CJIS) Security Policy (See Exhibit B) which includes authorized use of CHRI, dissemination of CHRI, statute authorization for civil applicant background checks conducted by noncriminal justice agencies, applicant notification and record challenge, security of CHRI, storage of CHRI, outsourcing of noncriminal justice administrative functions, and user fees. WSP will conduct regional audits of all agencies working under this MOU to ensure compliance to all state and federal standards.
- b. NCJA. The NCJA shall be responsible for ensuring:
  1. NCJA responds to requests for information by the FBI CJIS Division or the WSP in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of the agency.
  2. NCJA has formalized written procedures for the following, if applicable: criminal history use and dissemination, misuse, background checks, password management, storage, and destruction of CHRI.
  3. CHRI received as a result of licensing or employment purposes, pursuant to Public Law 92-544 is solely used for the purpose for which the record was requested. Subject fingerprints shall be submitted with all requests for CHRI for noncriminal justice purposes. Access to the FBI CJIS using name-based inquiry and record request messages is not permitted for noncriminal justice purpose, unless otherwise approved by the FBI.
  4. Access to CHRI by authorized officials is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or other authorized entities.

5. All fingerprint based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.
6. NCJA must notify the applicants fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The officials making the determination of suitability for licensing or employment shall provide the applicants the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record. These officials also must advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in Title 28, C.F.R. 16.34. Official making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so.
7. Appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity.
8. NCJA shall seek WSP permission prior to outsourcing noncriminal justice functions.
9. Outsourcing of noncriminal justice administrative functions requiring access to CHRI to either another governmental agency or a private contractor acting as an agent for the authorized receiving agency complies with the security and management control outsourcing standard for non-channelers (see Exhibit A).
10. NCJA is responsible for compliance to technical standards set forth by WSP and the CJIS Security Policy.
11. NCJA will conduct periodic self audits to ensure compliance with CJIS Security Policy.
12. NCJA will participate in WSP and FBI audits, provide plans for any compliance issues, and follow through to resolution within identified timeframes.
13. NCJA will ensure all appropriate staff members are trained according to the state and federal requirements.

### **III. CRIMINAL HISTORY RECORD INFORMATION RESPONSIBILITIES**

NCJA shall conform to system policies, as established by the FBI CJIS Division and WSP, before access to CHRI is permitted. This will allow for control over the data and give assurance of system security.

1. The rules and procedures governing access to CHRI shall apply equally to all participants in the system.
2. All noncriminal justice agencies with access to CHRI data must designate a specific unit, position, or personnel to access CHRI; noncriminal justice agencies must advise WSP of such personnel and changes to such designation.
3. All noncriminal justice agencies with access to CHRI data from the system shall permit an FBI CJIS Division or WSP audit team to conduct appropriate audits. NCJA must cooperate with these audits and respond promptly.

### **IV. SECURITY RESPONSIBILITIES**

#### **Technical Roles and Responsibilities**

NCJA must comply with and enforce system security. NCJA must have someone designated as the security point of contact (POC). Security POC's shall be responsible for the following:

1. Identifying the user of the hardware/software and ensuring that no unauthorized users have access to the same.
2. Identifying and documenting how the equipment is connected to the state system.

3. Ensuring that personnel security screening procedures are being followed as stated in the CJIS Security Policy.
4. Ensuring that appropriate hardware security measures are in place.
5. Supporting policy compliance and keeping the WSP informed of security incidents.
6. If the technical POC changes at your agency, notify WSP immediately.

#### **Security Enforcement**

NCJA is responsible for enforcing system security standards for their agency, in addition to all of the other agencies to which the NCJA provides CHRI information. Authorized users shall access and disseminate the CHRI data only for the purpose for which they are authorized. NCJA shall have a written policy for the discipline of policy violators.

#### **Technical Security Training**

All Information Technology (IT) employees who have access to and those who have direct responsibility to configure and maintain FBI CJIS systems must review security awareness training within six months of their appointment or assignment. Documentation pertaining to the materials used and those employees which receive security awareness training shall be maintained in a current status.

#### **Physical Security**

A physically secured location in a noncriminal justice facility, an area, a room, a group of rooms, that is/are subject to criminal justice agency management control security addendum and which contain hardware, software, and/or firmware (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch panels, etc.) that provide access to the CJIS sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that restrict unauthorized access.

All personnel with access to computer centers, CHRI, or areas where CHRI information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check. All personnel must review security awareness training within six months of their appointment or assignment.

#### **Personnel Security**

To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days of initial employment or assignment for all personnel who have authorized access to FBI CJIS information and those who have direct responsibility to configure and maintain computer systems and networks with access to FBI CJIS information. All requests from system access shall be made as specified by the CJIS Systems Officer (i.e. WSP Identification and Criminal History Section).

- c. NCJA shall use the data supplied by WSP and the FBI under this MOU only for the authorized purpose intended. NCJA shall not use this data for any other purpose and shall not disseminate this data with any other parties unless required by law. NCJA shall share any public disclosure requests regarding this data with the WSP.

#### **Storage**

Please see 'Security and Management Control Outsourcing Standard for Non-Channelers' (Exhibit A).

**V. LIAISON REPRESENTATIVES  
For the Washington State Patrol:**

Jim Anderson, Administrator  
Criminal Records Division  
PO Box 42619  
Olympia WA 98504-2619  
Phone: (360) 534-2101  
Fax: (360) 534-2070  
E-mail: [jim.anderson@wsp.wa.gov](mailto:jim.anderson@wsp.wa.gov)

**For the Island County**

**Housing Authority:**

~~Steve Gulliford~~ Teri Anania, EXECUTIVE DIRECTOR  
7 NW 6th St  
Coupeville WA 98239  
360-678-4181  
[teria@islandcountyha.org](mailto:teria@islandcountyha.org)

**VI. INDEMNIFICATION**

Each party shall defend, protect and hold harmless the other party from and against all claims, suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing this MOU.

**VII. PERIOD OF MOU**

This MOU becomes effective on the date of the last signature and continues for three years and may be renewed. It may be modified by mutual written consent of the two agencies. Liaison Representatives may modify Exhibit A by mutual written consent of the two agencies without changing the general conditions of this MOU.

**VIII. TERMINATION**

Except as otherwise provided in this MOU, either party may terminate this MOU upon ninety (90) days' written notification to the other party. If this MOU is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this MOU for performance prior to the effective date of termination.

**IX. DISPUTES**

In the event that a dispute arises under this MOU, it shall be determined in the following manner: The Chief of WSP, or designee, shall appoint one member to the Dispute Board. NCJA shall appoint one member to the Dispute Board. The Chief of WSP, or designee, and the NCJA shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. If applicable and as an alternative to this process, either of the parties may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.

**X. EXHIBITS**

The exhibits listed below are incorporated into and made a part of this MOU:

Exhibit A - 'Security and Management Control Outsourcing Standard for Non-Channelers'

Exhibit B - Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.2, published 8/9/2013 which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

**XI. ORDER OF PRECEDENCE**

In the event of any inconsistency in the terms of this MOU, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

- a. Applicable federal and state statutes and regulations;
- b. The Terms and Conditions contained in this MOU;
- c. The Exhibits attached to this MOU;
- d. Any other provisions of the MOU, whether incorporated by reference or otherwise.

**XII. ALL WRITINGS CONTAINED HEREIN**

This MOU contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this MOU shall be deemed to exist or to bind any of the parties hereto.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

ISLAND COUNTY  
HOUSING AUTHORITY

*John R. Batiste*  
 \_\_\_\_\_  
 John R. Batiste, Chief

*Teri Anania*  
 \_\_\_\_\_  
 Teri Anania, EXECUTIVE DIRECTOR

*9/18/13*  
 \_\_\_\_\_  
 Date

*9-16-2013*  
 \_\_\_\_\_  
 Date



## SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD for NON-CHANNELERS

The goal of this document is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the Contractor. Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security and Management Control Outsourcing Standard (Outsourcing Standard) is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI without a direct connection to the FBI CJIS Wide Area Network (WAN).

### 1.0 *Definitions*

- 1.01 *Access to CHRI* means to view or make use of CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by title 42, United States Code, section 14614(b).
- 1.02 *Authorized Recipient* means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.
- 1.03 *Chief Administrator* means the primary administrator of a Nonparty State’s criminal history record repository or a designee of such administrator who is

a regular full-time employee of the repository, which is also referred to as the State Identification Bureau (SIB) Chief.

- 1.04 *CHRI*, as referred to in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.
- 1.05 *Criminal History Record Check*, for purposes of this Outsourcing Standard only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.
- 1.06 *Compact Officer*, as provided in Article I(2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the compact among federal agencies], or (B) with respect to a Party State, the chief administrator of the State's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.
- 1.07 *Contractor* means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI.
- 1.08 *Dissemination* means the disclosure of CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 1.09 *Noncriminal Justice Administrative Functions* means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:
1. Making fitness determinations/recommendations
  2. Obtaining missing dispositions
  3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General
  4. Other authorized activities relating to the general handling, use, and storage of CHRI

- 1.10 *Noncriminal Justice Purposes*, as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.
- 1.11 *Outsourcing Standard* means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. This Outsourcing Standard authorizes access to CHRI for noncriminal justice purposes, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.
- 1.12 *Physically Secure Location* means a facility or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CHRI and associated information systems.
- 1.13 *Positive Identification*, as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints<sup>1</sup> or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other non-unique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.
- 1.14 *Public Carrier Network* means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: Dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.
- 1.15 *Security Violation* means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in

---

<sup>1</sup> The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning positive identification may be obtained from the FBI Compact Council office.

violation of: (A) Federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

2.0 *Responsibilities of the Authorized Recipient*

- 2.01 Prior to engaging in outsourcing any noncriminal justice administrative functions, the Authorized Recipient shall: (a) Request and receive written permission from (1) the State Compact Officer/Chief Administrator<sup>2</sup> or (2) the FBI Compact Officer<sup>3</sup>; (b) provide the Compact Officer/Chief Administrator copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested; and (c) inquire of the FBI Compact Officer whether a prospective Contractor has any security violations (See Section 8.04). The FBI Compact Officer will report those findings to the Authorized Recipient and, when applicable, to the State Compact Officer/Chief Administrator.
- 2.02 The Authorized Recipient shall execute a contract or agreement prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.
- 2.03 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; limit retention of the information to a period of time not to exceed that period of time the Authorized Recipient is permitted to retain such information; prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General; ensure the security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; and ensure that Contractor

---

<sup>2</sup>The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and Authorized Recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.

<sup>3</sup>State or local Authorized Recipients based on State or Federal Statutes shall contact the State Compact Officer/Chief Administrator. Federal or Regulatory Agency Authorized Recipients shall contact the FBI Compact Officer.

personnel comply with this Outsourcing Standard.

- a. The Authorized Recipient shall conduct criminal history record checks of Contractor personnel having access to CHRI if such checks are required or authorized of the Authorized Recipient's personnel having similar access.<sup>4</sup> The Authorized Recipient shall maintain updated records of Contractor personnel who have access to CHRI and update those records within 24 hours when changes to that access occur and, if a criminal history record check is required, the Authorized Recipient shall maintain a list of Contractor personnel who successfully completed the criminal history record check.
  - b. The Authorized Recipient shall ensure that the Contractor maintains site security.
  - c. The Authorized Recipient shall ensure that the most current version of both the Outsourcing Standard and the CJIS Security Policy are incorporated by reference at the time of contract, contract renewal, or within 30 calendar days (unless otherwise directed) of notification of successor versions of the Outsourcing Standard and/or CJIS Security Policy, whichever is sooner. The Authorized Recipient shall notify the Contractor within 30 calendar days (unless otherwise directed) of FBI notification regarding changes or updates to the Outsourcing Standard and/or CJIS Security Policy.
- 2.04 The Authorized Recipient shall understand the communications and record capabilities of the Contractor which has access to federal or state records through, or because of, its outsourcing relationship with the Authorized Recipient. The Authorized Recipient shall maintain an updated topological drawing which depicts the interconnectivity of the Contractor's network configuration.
- 2.05 The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the Outsourcing Standard. The Authorized Recipient shall certify to the Compact Officer/Chief Administrator that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.

---

<sup>4</sup>If a national criminal history record check of Authorized Recipient personnel having access to CHRI is mandated or authorized by a federal statute, executive order, or state statute approved by the Attorney General under Public Law 92-544, the State Compact Officer/Chief Administrator and/or the FBI Compact Officer must ensure Contractor personnel having similar access are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives. The national criminal history record checks of Contractor personnel with access to CHRI cannot be outsourced and must be performed by the Authorized Recipient.

2.06 The Authorized Recipient shall provide written notice of any early voluntary termination of the contract to the Compact Officer/Chief Administrator or the FBI Compact Officer.

3.0 *Responsibilities of the Contractor*

3.01 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the CJIS Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

3.02 The Contractor shall develop, document, administer, and maintain a Security Program (Physical, Personnel, and Information Technology) to comply with the most current Outsourcing Standard and the most current FBI *CJIS Security Policy*. The Security Program shall describe the implementation of the security requirements described in this Outsourcing Standard and the FBI *CJIS Security Policy*. In addition, the Contractor is also responsible to set, maintain, and enforce the standards for the selection, supervision, and separation of personnel who have access to CHRI. The Authorized Recipient shall provide the written approval of a Contractor's Security Program.

3.03 The requirements for a Security Program should include, at a minimum:

- a) Description of the implementation of the security requirements described in this Outsourcing Standard and the *CJIS Security Policy*.
- b) Security Training.
- c) Guidelines for documentation of security violations.
- d) Standards for the selection, supervision, and separation of personnel with access to CHRI.

\*\*If the Contractor is using a corporate policy, it must meet the requirements outlined in this Outsourcing Standard and the *CJIS Security Policy*. If the corporate policy is not this specific, it must flow down to a level where the documentation supports these requirements.

3.04 Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. The Authorized Recipient shall review and provide to the Contractor written approval of the Security Training Program. Training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall annually, not later than the anniversary date of the contract, certify in writing to the Authorized Recipient that annual refresher training was completed for those Contractor personnel with access

to CHRI.

- 3.05 The Contractor shall make its facilities available for announced and unannounced audits performed by the Authorized Recipient, the state, or the FBI on behalf of the Compact Council.
- 3.06 The Contractor's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI CJIS Division. During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.
- 3.07 The Contractor shall maintain CHRI only for the period of time necessary to fulfill its contractual obligations but not to exceed the period of time that the Authorized Recipient is authorized to maintain and does maintain the CHRI.
- 3.08 The Contractor shall maintain a log of any dissemination of CHRI, for a minimum of 365 days.

#### 4.0 *Site Security*

- 4.01 The Authorized Recipient shall ensure that the Contractor site(s) is a physically secure location to protect against any unauthorized access to CHRI.

#### 5.0 *Dissemination*

- 5.01 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 5.02 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) The Authorized Recipient and the secondary recipient with unique identifiers, (B) the record disseminated, (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.
- 5.03 If CHRI is stored or disseminated in an electronic format, the Contractor shall protect against unauthorized access to the equipment and any of the data. In no event shall responses containing CHRI be disseminated other than as governed by this Outsourcing Standard or more stringent contract requirements.

#### 6.0 *Personnel Security*

- 6.01 If a local, state, or federal written standard requires or authorizes a criminal history record check of the Authorized Recipient's personnel with access to

CHRI, then a criminal history record check shall be required of the Contractor's (and approved Sub-Contractor's) employees having access to CHRI. Criminal history record checks of Contractor and approved Sub-Contractor employees, at a minimum, will be no less stringent than criminal history record checks that are performed on the Authorized Recipient's personnel performing similar functions. Criminal history record checks must be completed prior to accessing CHRI under the contract.

- 6.02 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm in writing that each employee has certified in writing that he/she understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities. The Contractor shall maintain the employee certifications in a file that is subject to review during audits. Employees shall make such certification prior to performing work under the contract.
- 6.03 The Contractor shall maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur, and if a criminal history record check is required, maintain a list of personnel who have successfully completed criminal history record checks. The Contractor shall notify Authorized Recipients within 24 hours when additions or deletions occur.

## 7.0 *System Security*

- 7.01 The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy.
  - a. If CHRI can be accessed by unauthorized personnel via Wide Area Network/Local Area Network or the Internet, then the Contractor shall protect the CHRI with firewall-type devices to prevent such unauthorized access. These devices shall implement a minimum firewall profile as specified by the CJIS Security Policy in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.
  - b. Data encryption shall be required throughout the network passing CHRI through a shared public carrier network.
- 7.02 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.
  - a. CHRI shall be stored in a physically secure location.
  - b. The Authorized Recipient shall ensure that a procedure is in place for



sanitizing all fixed storage media (e.g., disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal, or reuse. Sanitization procedures include overwriting the media and/or degaussing the media.

- c. The Authorized Recipient shall ensure that a procedure is in place for the disposal or return of all non-fixed storage media (e.g., hard copies, print-outs).

7.03 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient, Contractor, or sub-Contractor must be assigned a unique identifying number.

## 8.0 *Security Violations*

### 8.01 Duties of the Authorized Recipient and Contractor

- a. The Contractor shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference.
- b. Pending investigation, the Contractor shall, upon detection or awareness, suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.
- c. The Contractor shall immediately (within four hours) notify the Authorized Recipient of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. Within five calendar days of such notification, the Contractor shall provide the Authorized Recipient a written report documenting such security violation, any corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.
- d. The Authorized Recipient shall immediately (within four hours) notify the State Compact Officer/Chief Administrator and the FBI Compact Officer of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator, if applicable, and the FBI Compact Officer, within five calendar days of receipt of the written report from the Contractor. The written report must include any corrective actions taken by the Contractor and the Authorized Recipient to resolve such security violation.

- 8.02 Termination of the contract by the Authorized Recipient for security violations
- a. The contract is subject to termination by the Authorized Recipient for security violations involving CHRI obtained pursuant to the contract.
  - b. The contract is subject to termination by the Authorized Recipient for the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.
  - c. If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient shall terminate the contract.
- 8.03 Suspension or termination of the exchange of CHRI for security violations
- a. Notwithstanding the actions taken by the State Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Compact Council or the United States Attorney General may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 CFR §906.2(d).
  - b. If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United States Attorney General by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be deleted or returned in accordance with the provisions and time frame as specified by the Authorized Recipient.
- 8.04 The Authorized Recipient shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following:
- a. The termination of a contract for security violations.
  - b. Security violations involving the unauthorized access to CHRI.
  - c. The Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.
- 8.05 The Compact Officer/Chief Administrator, Compact Council and the United States Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.
- 8.06 The Compact Officer/Chief Administrator, Compact Council, and the United

States Attorney General reserve the right to audit the Authorized Recipient and the Contractor's operations and procedures at scheduled or unscheduled times. The Compact Council, the United States Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the contract.

#### 9.0 *Miscellaneous Provisions*

- 9.01 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, Compact Officer/Chief Administrator (where applicable), and the FBI.
- 9.02 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) The CJIS Security Policy.
- 9.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and the CHRI accessed therefrom and it is understood that there may be terms and conditions of the appended contract which impose more stringent requirements upon the Contractor.<sup>5</sup>
- 9.04 The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. Conformance to such security measures may not be less stringent than stated in this Outsourcing Standard without the consent of the Compact Council in consultation with the United States Attorney General.
- 9.05 This Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.
- 9.06 Appropriate notices, assurances, and correspondence to the FBI Compact Officer, Compact Council, and the United States Attorney General required by Section 8.0 of this Outsourcing Standard shall be forwarded by First Class Mail to:
  - FBI Compact Officer
  - 1000 Custer Hollow Road
  - Module D-3
  - Clarksburg, WV 26306

#### 10.0 *Exemption from Above Provisions*

---

<sup>5</sup>Such conditions could include additional audits, fees, or security requirements. The Compact Council, Authorized Recipients, and the Compact Officer/Chief Administrator have the explicit authority to require more stringent standards than those contained in the Outsourcing Standard.

- 10.01 An Information Technology (IT) contract need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:
1. Access to CHRI by the IT contractor's personnel is limited solely for the development and/or maintenance of the Authorized Recipient's computer system;
  2. Access to CHRI is incidental, but necessary, to the duties being performed by the IT contractor;
  3. The computer system resides within the Authorized Recipient's facility;
  4. The Authorized Recipient's personnel supervise or work directly with the IT contractor personnel;
  5. The Authorized Recipient maintains complete, positive control of the IT contractor's access to the computer system and CHRI contained therein; and
  6. The Authorized Recipient retains all of the duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard.

10.02 An Authorized Recipient's contract where access to CHRI is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 4.0, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:

1. Access to CHRI by the Contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient;
2. Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor;

3. The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the Authorized Recipient;
4. The Contractor's personnel are subject to the same criminal history record checks as the Authorized Recipient's personnel;
5. The criminal history record checks of the Contractor personnel are completed prior to work on the contract or agreement;
6. The Authorized Recipient retains all other duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard; and
7. The Contractor stores the CHRI in a physically secure location.

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above referenced Contract between the Washington State Patrol and the Island County Housing Authority is hereby amended as follows:

- The end date shall be extended through September 17, 2021.
- EXHIBIT B CJIS Security Policy 5.1 shall be replaced with EXHIBIT B CJIS Security Policy 5.5.

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

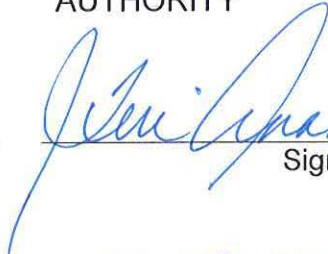
STATE OF WASHINGTON  
WASHINGTON STATE PATROL

ISLAND COUNTY HOUSING  
AUTHORITY



FOR: John R. Batiste, Chief

1/3/2017  
Date



Signature

EXECUTIVE DIRECTOR  
HOUSING AUTHORITY OF  
Island County

12-27-2016

Date

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above referenced Contract between the Washington State Patrol and the Pierce County Housing Authority is hereby amended as follows:

- The end date shall be extended through September 25, 2021.
- EXHIBIT B CJIS Security Policy 5.1 shall be replaced with EXHIBIT B CJIS Security Policy 5.5.

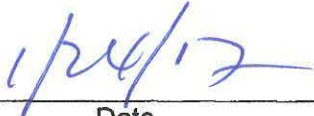
All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

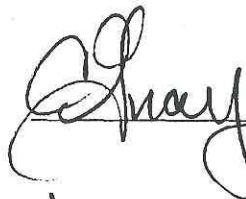
STATE OF WASHINGTON  
WASHINGTON STATE PATROL



FOR: John R. Batiste, Chief

  
Date

PIERCE COUNTY HOUSING  
AUTHORITY



Signature

  
Date

JAY INSLEE  
Governor



JOHN R. BATISTE  
Chief

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

General Administration Building • PO BOX 42602 • Olympia, WA 98504-2602 • (360) 596-4043 • www.wsp.wa.gov

October 14, 2013

Ms. Tamara Meade  
Pierce Co Housing Authority  
PO Box 45410  
Tacoma WA 98448-0410

Subject: WSP Agreement No. C130756GSC

Enclosed with this letter is one fully executed original of the referenced agreement between the Washington State Patrol and your agency. Please keep this original for your records.

The Washington State Patrol contract tracking number is the agreement number referenced above; please use this number on all correspondence regarding this agreement. If you need further assistance, please contact Ms. Cindy Haider at Budget and Fiscal Services, (360) 596-4071.

Sincerely,

A handwritten signature in cursive script that reads "Cindy Haider".

for, Mr. Robert L. Maki, CFE, CGFM  
Budget and Fiscal Services

RLM:clh  
Enclosure

**MAILED**  
10/15/13





RECEIVED  
SEP 12 2013  
PIERCE COUNTY HOUSING AUTH

**MEMORANDUM OF UNDERSTANDING**

**Between the**

**WASHINGTON STATE PATROL**

**And the**

**PIERCE COUNTY  
HOUSING AUTHORITY**

**I. PURPOSE**

The parties to this Memorandum of Understanding (MOU) are the Washington State Patrol, Identification and Criminal History Section (WSP) and the Pierce County Housing Authority, a non criminal justice agency (NCJA). This MOU sets forth the policy to ensure the protection of criminal history record information (CHRI) between the WSP, the NCJA, and the Federal Bureau of Investigation (FBI). This MOU provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CHRI data. This policy applies to the NCJA and its contractors with access to, or who operate in support of, non-criminal justice services and information.

**II. ADMINISTRATIVE RESPONSIBILITIES**

As participants in this MOU, the parties will develop mutually and separately appropriate procedures for transmission, dissemination, storage, and destruction of CHRI data.

- a. The Washington State Patrol. WSP shall ensure the NCJA complies with the Criminal Justice Information Services (CJIS) Security Policy (See Exhibit B) which includes authorized use of CHRI, dissemination of CHRI, statute authorization for civil applicant background checks conducted by noncriminal justice agencies, applicant notification and record challenge, security of CHRI, storage of CHRI, outsourcing of noncriminal justice administrative functions, and user fees. WSP will conduct regional audits of all agencies working under this MOU to ensure compliance to all state and federal standards.
- b. NCJA. The NCJA shall be responsible for ensuring:
  1. NCJA responds to requests for information by the FBI CJIS Division or the WSP in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of the agency.
  2. NCJA has formalized written procedures for the following, if applicable: criminal history use and dissemination, misuse, background checks, password management, storage, and destruction of CHRI.
  3. CHRI received as a result of licensing or employment purposes, pursuant to Public Law 92-544 is solely used for the purpose for which the record was requested. Subject fingerprints shall be submitted with all requests for CHRI for noncriminal justice purposes. Access to the FBI CJIS using name-based inquiry and record request messages is not permitted for noncriminal justice purpose, unless otherwise approved by the FBI.
  4. Access to CHRI by authorized officials is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or other authorized entities.

5. All fingerprint based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.
6. NCJA must notify the applicants fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The officials making the determination of suitability for licensing or employment shall provide the applicants the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record. These officials also must advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in Title 28, C.F.R. 16.34. Official making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so.
7. Appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity.
8. NCJA shall seek WSP permission prior to outsourcing noncriminal justice functions.
9. Outsourcing of noncriminal justice administrative functions requiring access to CHRI to either another governmental agency or a private contractor acting as an agent for the authorized receiving agency complies with the security and management control outsourcing standard for non-channelers (see Exhibit A).
10. NCJA is responsible for compliance to technical standards set forth by WSP and the CJIS Security Policy.
11. NCJA will conduct periodic self audits to ensure compliance with CJIS Security Policy.
12. NCJA will participate in WSP and FBI audits, provide plans for any compliance issues, and follow through to resolution within identified timeframes.
13. NCJA will ensure all appropriate staff members are trained according to the state and federal requirements.

### **III. CRIMINAL HISTORY RECORD INFORMATION RESPONSIBILITIES**

NCJA shall conform to system policies, as established by the FBI CJIS Division and WSP, before access to CHRI is permitted. This will allow for control over the data and give assurance of system security.

1. The rules and procedures governing access to CHRI shall apply equally to all participants in the system.
2. All noncriminal justice agencies with access to CHRI data must designate a specific unit, position, or personnel to access CHRI; noncriminal justice agencies must advise WSP of such personnel and changes to such designation.
3. All noncriminal justice agencies with access to CHRI data from the system shall permit an FBI CJIS Division or WSP audit team to conduct appropriate audits. NCJA must cooperate with these audits and respond promptly.

### **IV. SECURITY RESPONSIBILITIES**

#### **Technical Roles and Responsibilities**

NCJA must comply with and enforce system security. NCJA must have someone designated as the security point of contact (POC). Security POC's shall be responsible for the following:

1. Identifying the user of the hardware/software and ensuring that no unauthorized users have access to the same.
2. Identifying and documenting how the equipment is connected to the state system.

3. Ensuring that personnel security screening procedures are being followed as stated in the CJIS Security Policy.
4. Ensuring that appropriate hardware security measures are in place.
5. Supporting policy compliance and keeping the WSP informed of security incidents.
6. If the technical POC changes at your agency, notify WSP immediately.

#### **Security Enforcement**

NCJA is responsible for enforcing system security standards for their agency, in addition to all of the other agencies to which the NCJA provides CHRI information. Authorized users shall access and disseminate the CHRI data only for the purpose for which they are authorized. NCJA shall have a written policy for the discipline of policy violators.

#### **Technical Security Training**

All Information Technology (IT) employees who have access to and those who have direct responsibility to configure and maintain FBI CJIS systems must review security awareness training within six months of their appointment or assignment. Documentation pertaining to the materials used and those employees which receive security awareness training shall be maintained in a current status.

#### **Physical Security**

A physically secured location in a noncriminal justice facility, an area, a room, a group of rooms, that is/are subject to criminal justice agency management control security addendum and which contain hardware, software, and/or firmware (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch panels, etc.) that provide access to the CJIS sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that restrict unauthorized access.

All personnel with access to computer centers, CHRI, or areas where CHRI information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check. All personnel must review security awareness training within six months of their appointment or assignment.

#### **Personnel Security**

To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days of initial employment or assignment for all personnel who have authorized access to FBI CJIS information and those who have direct responsibility to configure and maintain computer systems and networks with access to FBI CJIS information. All requests from system access shall be made as specified by the CJIS Systems Officer (i.e. WSP Identification and Criminal History Section).

- c. NCJA shall use the data supplied by WSP and the FBI under this MOU only for the authorized purpose intended. NCJA shall not use this data for any other purpose and shall not disseminate this data with any other parties unless required by law. NCJA shall share any public disclosure requests regarding this data with the WSP.

#### **Storage**

Please see 'Security and Management Control Outsourcing Standard for Non-Channelers' (Exhibit A).

**V. LIAISON REPRESENTATIVES**  
**For the Washington State Patrol:**

Jim Anderson, Administrator  
Criminal Records Division  
PO Box 42619  
Olympia WA 98504-2619  
Phone: (360) 534-2101  
Fax:(360) 534-2070  
E-mail: [jim.anderson@wsp.wa.gov](mailto:jim.anderson@wsp.wa.gov)

**For the Pierce County  
Housing Authority:**  
Tamara Meade  
PO Box 45410  
Tacoma WA 98445  
253-620-5420  
[tamaramede@pchawa.org](mailto:tamaramede@pchawa.org)

**VI. INDEMNIFICATION**

Each party shall defend, protect and hold harmless the other party from and against all claims, suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing this MOU.

**VII. PERIOD OF MOU**

This MOU becomes effective on the date of the last signature and continues for three years and may be renewed. It may be modified by mutual written consent of the two agencies. Liaison Representatives may modify Exhibit A by mutual written consent of the two agencies without changing the general conditions of this MOU.

**VIII. TERMINATION**

Except as otherwise provided in this MOU, either party may terminate this MOU upon ninety (90) days' written notification to the other party. If this MOU is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this MOU for performance prior to the effective date of termination.

**IX. DISPUTES**

In the event that a dispute arises under this MOU, it shall be determined in the following manner: The Chief of WSP, or designee, shall appoint one member to the Dispute Board. NCJA shall appoint one member to the Dispute Board. The Chief of WSP, or designee, and the NCJA shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. If applicable and as an alternative to this process, either of the parties may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.

**X. EXHIBITS**

The exhibits listed below are incorporated into and made a part of this MOU:

Exhibit A - 'Security and Management Control Outsourcing Standard for Non-Channelers'

Exhibit B - Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.2, published 8/9/2013 which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

**XI. ORDER OF PRECEDENCE**

In the event of any inconsistency in the terms of this MOU, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

- a. Applicable federal and state statutes and regulations;
- b. The Terms and Conditions contained in this MOU;
- c. The Exhibits attached to this MOU;
- d. Any other provisions of the MOU, whether incorporated by reference or otherwise.

**XII. ALL WRITINGS CONTAINED HEREIN**

This MOU contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this MOU shall be deemed to exist or to bind any of the parties hereto.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL



John R. Batiste, Chief

Date

9/26/13

PIERCE COUNTY  
HOUSING AUTHORITY



Date

9/13/13

**MEMORANDUM OF UNDERSTANDING**

**Between the**

**WASHINGTON STATE PATROL**

**And the**

**QUILEUTE HOUSING AUTHORITY**

**I. PURPOSE**

The parties to this Memorandum of Understanding (MOU) are the Washington State Patrol, Identification and Criminal History Section (WSP) and the Quileute Housing Authority, a non criminal justice agency (NCJA). This MOU sets forth the policy to ensure the protection of criminal history record information (CHRI) between the WSP, the NCJA, and the Federal Bureau of Investigation (FBI). This MOU provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CHRI data. This policy applies to the NCJA and its contractors with access to, or who operate in support of, non-criminal justice services and information.

**II. ADMINISTRATIVE RESPONSIBILITIES**

As participants in this MOU, the parties will develop mutually and separately appropriate procedures for transmission, dissemination, storage, and destruction of CHRI data.

- a. The Washington State Patrol. WSP shall ensure the NCJA complies with the Criminal Justice Information Services (CJIS) Security Policy (See Exhibit B) which includes authorized use of CHRI, dissemination of CHRI, statute authorization for civil applicant background checks conducted by noncriminal justice agencies, applicant notification and record challenge, security of CHRI, storage of CHRI, outsourcing of noncriminal justice administrative functions, and user fees. WSP will conduct regional audits of all agencies working under this MOU to ensure compliance to all state and federal standards.
- b. NCJA. The NCJA shall be responsible for ensuring:
  1. NCJA responds to requests for information by the FBI CJIS Division or the WSP in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of the agency.
  2. NCJA has formalized written procedures for the following, if applicable: criminal history use and dissemination, misuse, background checks, password management, storage, and destruction of CHRI.
  3. CHRI received as a result of licensing or employment purposes, pursuant to Public Law 92-544 is solely used for the purpose for which the record was requested. Subject fingerprints shall be submitted with all requests for CHRI for noncriminal justice purposes. Access to the FBI CJIS using name-based inquiry and record request messages is not permitted for noncriminal justice purpose, unless otherwise approved by the FBI.
  4. Access to CHRI by authorized officials is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or other authorized entities.

5. All fingerprint based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.
6. NCJA must notify the applicants fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The officials making the determination of suitability for licensing or employment shall provide the applicants the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record. These officials also must advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in Title 28, C.F.R. 16.34. Official making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so.
7. Appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity.
8. NCJA shall seek WSP permission prior to outsourcing noncriminal justice functions.
9. Outsourcing of noncriminal justice administrative functions requiring access to CHRI to either another governmental agency or a private contractor acting as an agent for the authorized receiving agency complies with the security and management control outsourcing standard for non-channelers (see Exhibit A).
10. NCJA is responsible for compliance to technical standards set forth by WSP and the CJIS Security Policy.
11. NCJA will conduct periodic self audits to ensure compliance with CJIS Security Policy.
12. NCJA will participate in WSP and FBI audits, provide plans for any compliance issues, and follow through to resolution within identified timeframes.
13. NCJA will ensure all appropriate staff members are trained according to the state and federal requirements.

### **III. CRIMINAL HISTORY RECORD INFORMATION RESPONSIBILITIES**

NCJA shall conform to system policies, as established by the FBI CJIS Division and WSP, before access to CHRI is permitted. This will allow for control over the data and give assurance of system security.

1. The rules and procedures governing access to CHRI shall apply equally to all participants in the system.
2. All noncriminal justice agencies with access to CHRI data must designate a specific unit, position, or personnel to access CHRI; noncriminal justice agencies must advise WSP of such personnel and changes to such designation.
3. All noncriminal justice agencies with access to CHRI data from the system shall permit an FBI CJIS Division or WSP audit team to conduct appropriate audits. NCJA must cooperate with these audits and respond promptly.

### **IV. SECURITY RESPONSIBILITIES**

#### **Technical Roles and Responsibilities**

NCJA must comply with and enforce system security. NCJA must have someone designated as the security point of contact (POC). Security POC's shall be responsible for the following:

1. Identifying the user of the hardware/software and ensuring that no unauthorized users have access to the same.
2. Identifying and documenting how the equipment is connected to the state system.

3. Ensuring that personnel security screening procedures are being followed as stated in the CJIS Security Policy.
4. Ensuring that appropriate hardware security measures are in place.
5. Supporting policy compliance and keeping the WSP informed of security incidents.
6. If the technical POC changes at your agency, notify WSP immediately.

#### **Security Enforcement**

NCJA is responsible for enforcing system security standards for their agency, in addition to all of the other agencies to which the NCJA provides CHRI information. Authorized users shall access and disseminate the CHRI data only for the purpose for which they are authorized. NCJA shall have a written policy for the discipline of policy violators.

#### **Technical Security Training**

All Information Technology (IT) employees who have access to and those who have direct responsibility to configure and maintain FBI CJIS systems must review security awareness training within six months of their appointment or assignment. Documentation pertaining to the materials used and those employees which receive security awareness training shall be maintained in a current status.

#### **Physical Security**

A physically secured location in a noncriminal justice facility, an area, a room, a group of rooms, that is/are subject to criminal justice agency management control security addendum and which contain hardware, software, and/or firmware (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch panels, etc.) that provide access to the CJIS sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that restrict unauthorized access.

All personnel with access to computer centers, CHRI, or areas where CHRI information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check. All personnel must review security awareness training within six months of their appointment or assignment.

#### **Personnel Security**

To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days of initial employment or assignment for all personnel who have authorized access to FBI CJIS information and those who have direct responsibility to configure and maintain computer systems and networks with access to FBI CJIS information. All requests from system access shall be made as specified by the CJIS Systems Officer (i.e. WSP Identification and Criminal History Section).

- c. NCJA shall use the data supplied by WSP and the FBI under this MOU only for the authorized purpose intended. NCJA shall not use this data for any other purpose and shall not disseminate this data with any other parties unless required by law. NCJA shall share any public disclosure requests regarding this data with the WSP.

#### **Storage**

Please see 'Security and Management Control Outsourcing Standard for Non-Channelers' (Exhibit A).



**V. LIAISON REPRESENTATIVES**

**For the Washington State Patrol:**

Jim Anderson, Administrator  
Criminal Records Division  
PO Box 42619  
Olympia WA 98504-2619  
Phone: (360) 534-2101  
Fax: (360) 534-2070  
E-mail: [jim.anderson@wsp.wa.gov](mailto:jim.anderson@wsp.wa.gov)

**For the Quileute Housing Authority:**

Ruth Jackson  
PO Box 159  
La Push WA 98350  
360-374-9719  
[ruth.jackson@quileutenation.org](mailto:ruth.jackson@quileutenation.org)

**VI. INDEMNIFICATION**

Each party shall defend, protect and hold harmless the other party from and against all claims, suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing this MOU.

**VII. PERIOD OF MOU**

This MOU becomes effective on the date of the last signature and continues for three years and may be renewed. It may be modified by mutual written consent of the two agencies. Liaison Representatives may modify Exhibit A by mutual written consent of the two agencies without changing the general conditions of this MOU.

**VIII. TERMINATION**

Except as otherwise provided in this MOU, either party may terminate this MOU upon ninety (90) days' written notification to the other party. If this MOU is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this MOU for performance prior to the effective date of termination.

**IX. DISPUTES**

In the event that a dispute arises under this MOU, it shall be determined in the following manner: The Chief of WSP, or designee, shall appoint one member to the Dispute Board. NCJA shall appoint one member to the Dispute Board. The Chief of WSP, or designee, and the NCJA shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. If applicable and as an alternative to this process, either of the parties may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.

**X. EXHIBITS**

The exhibits listed below are incorporated into and made a part of this MOU:

Exhibit A - 'Security and Management Control Outsourcing Standard for Non-Channelers'

Exhibit B - Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.2, published 8/9/2013 which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

**XI. ORDER OF PRECEDENCE**


In the event of any inconsistency in the terms of this MOU, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

- a. Applicable federal and state statutes and regulations;
- b. The Terms and Conditions contained in this MOU;
- c. The Exhibits attached to this MOU;
- d. Any other provisions of the MOU, whether incorporated by reference or otherwise.

**XII. ALL WRITINGS CONTAINED HEREIN**

This MOU contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this MOU shall be deemed to exist or to bind any of the parties hereto.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

  
\_\_\_\_\_  
John R. Batiste, Chief

9/20/13  
Date

QUILEUTE HOUSING AUTHORITY

  
\_\_\_\_\_  
ANNA PARRIS - Exec DIR

9/17/2013  
Date

## SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD for NON-CHANNELERS

The goal of this document is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the Contractor. Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security and Management Control Outsourcing Standard (Outsourcing Standard) is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI without a direct connection to the FBI CJIS Wide Area Network (WAN).

### 1.0 *Definitions*

- 1.01 *Access to CHRI* means to view or make use of CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by title 42, United States Code, section 14614(b).
- 1.02 *Authorized Recipient* means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.
- 1.03 *Chief Administrator* means the primary administrator of a Nonparty State’s criminal history record repository or a designee of such administrator who is

a regular full-time employee of the repository, which is also referred to as the State Identification Bureau (SIB) Chief.

- 1.04 *CHRI*, as referred to in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.
- 1.05 *Criminal History Record Check*, for purposes of this Outsourcing Standard only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.
- 1.06 *Compact Officer*, as provided in Article I(2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the compact among federal agencies], or (B) with respect to a Party State, the chief administrator of the State's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.
- 1.07 *Contractor* means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI.
- 1.08 *Dissemination* means the disclosure of CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 1.09 *Noncriminal Justice Administrative Functions* means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:
1. Making fitness determinations/recommendations
  2. Obtaining missing dispositions
  3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General
  4. Other authorized activities relating to the general handling, use, and storage of CHRI

- 1.10 *Noncriminal Justice Purposes*, as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.
- 1.11 *Outsourcing Standard* means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. This Outsourcing Standard authorizes access to CHRI for noncriminal justice purposes, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.
- 1.12 *Physically Secure Location* means a facility or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CHRI and associated information systems.
- 1.13 *Positive Identification*, as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints<sup>1</sup> or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other non-unique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.
- 1.14 *Public Carrier Network* means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: Dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.
- 1.15 *Security Violation* means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in

---

<sup>1</sup> The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning positive identification may be obtained from the FBI Compact Council office.

violation of: (A) Federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

2.0 *Responsibilities of the Authorized Recipient*

- 2.01 Prior to engaging in outsourcing any noncriminal justice administrative functions, the Authorized Recipient shall: (a) Request and receive written permission from (1) the State Compact Officer/Chief Administrator<sup>2</sup> or (2) the FBI Compact Officer<sup>3</sup>; (b) provide the Compact Officer/Chief Administrator copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested; and (c) inquire of the FBI Compact Officer whether a prospective Contractor has any security violations (See Section 8.04). The FBI Compact Officer will report those findings to the Authorized Recipient and, when applicable, to the State Compact Officer/Chief Administrator.
- 2.02 The Authorized Recipient shall execute a contract or agreement prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.
- 2.03 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; limit retention of the information to a period of time not to exceed that period of time the Authorized Recipient is permitted to retain such information; prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General; ensure the security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; and ensure that Contractor

---

<sup>2</sup>The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and Authorized Recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.

<sup>3</sup>State or local Authorized Recipients based on State or Federal Statutes shall contact the State Compact Officer/Chief Administrator. Federal or Regulatory Agency Authorized Recipients shall contact the FBI Compact Officer.

personnel comply with this Outsourcing Standard.

- a. The Authorized Recipient shall conduct criminal history record checks of Contractor personnel having access to CHRI if such checks are required or authorized of the Authorized Recipient's personnel having similar access.<sup>4</sup> The Authorized Recipient shall maintain updated records of Contractor personnel who have access to CHRI and update those records within 24 hours when changes to that access occur and, if a criminal history record check is required, the Authorized Recipient shall maintain a list of Contractor personnel who successfully completed the criminal history record check.
  - b. The Authorized Recipient shall ensure that the Contractor maintains site security.
  - c. The Authorized Recipient shall ensure that the most current version of both the Outsourcing Standard and the CJIS Security Policy are incorporated by reference at the time of contract, contract renewal, or within 30 calendar days (unless otherwise directed) of notification of successor versions of the Outsourcing Standard and/or CJIS Security Policy, whichever is sooner. The Authorized Recipient shall notify the Contractor within 30 calendar days (unless otherwise directed) of FBI notification regarding changes or updates to the Outsourcing Standard and/or CJIS Security Policy.
- 2.04 The Authorized Recipient shall understand the communications and record capabilities of the Contractor which has access to federal or state records through, or because of, its outsourcing relationship with the Authorized Recipient. The Authorized Recipient shall maintain an updated topological drawing which depicts the interconnectivity of the Contractor's network configuration.
- 2.05 The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the Outsourcing Standard. The Authorized Recipient shall certify to the Compact Officer/Chief Administrator that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.

---

<sup>4</sup>If a national criminal history record check of Authorized Recipient personnel having access to CHRI is mandated or authorized by a federal statute, executive order, or state statute approved by the Attorney General under Public Law 92-544, the State Compact Officer/Chief Administrator and/or the FBI Compact Officer must ensure Contractor personnel having similar access are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives. The national criminal history record checks of Contractor personnel with access to CHRI cannot be outsourced and must be performed by the Authorized Recipient.

2.06 The Authorized Recipient shall provide written notice of any early voluntary termination of the contract to the Compact Officer/Chief Administrator or the FBI Compact Officer.

3.0 *Responsibilities of the Contractor*

3.01 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the CJIS Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

3.02 The Contractor shall develop, document, administer, and maintain a Security Program (Physical, Personnel, and Information Technology) to comply with the most current Outsourcing Standard and the most current FBI *CJIS Security Policy*. The Security Program shall describe the implementation of the security requirements described in this Outsourcing Standard and the FBI *CJIS Security Policy*. In addition, the Contractor is also responsible to set, maintain, and enforce the standards for the selection, supervision, and separation of personnel who have access to CHRI. The Authorized Recipient shall provide the written approval of a Contractor's Security Program.

3.03 The requirements for a Security Program should include, at a minimum:

- a) Description of the implementation of the security requirements described in this Outsourcing Standard and the *CJIS Security Policy*.
- b) Security Training.
- c) Guidelines for documentation of security violations.
- d) Standards for the selection, supervision, and separation of personnel with access to CHRI.

\*\*If the Contractor is using a corporate policy, it must meet the requirements outlined in this Outsourcing Standard and the *CJIS Security Policy*. If the corporate policy is not this specific, it must flow down to a level where the documentation supports these requirements.

3.04 Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. The Authorized Recipient shall review and provide to the Contractor written approval of the Security Training Program. Training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall annually, not later than the anniversary date of the contract, certify in writing to the Authorized Recipient that annual refresher training was completed for those Contractor personnel with access



to CHRI.

- 3.05 The Contractor shall make its facilities available for announced and unannounced audits performed by the Authorized Recipient, the state, or the FBI on behalf of the Compact Council.
- 3.06 The Contractor's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI CJIS Division. During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.
- 3.07 The Contractor shall maintain CHRI only for the period of time necessary to fulfill its contractual obligations but not to exceed the period of time that the Authorized Recipient is authorized to maintain and does maintain the CHRI.
- 3.08 The Contractor shall maintain a log of any dissemination of CHRI, for a minimum of 365 days.

#### 4.0 *Site Security*

- 4.01 The Authorized Recipient shall ensure that the Contractor site(s) is a physically secure location to protect against any unauthorized access to CHRI.

#### 5.0 *Dissemination*

- 5.01 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 5.02 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) The Authorized Recipient and the secondary recipient with unique identifiers, (B) the record disseminated, (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.
- 5.03 If CHRI is stored or disseminated in an electronic format, the Contractor shall protect against unauthorized access to the equipment and any of the data. In no event shall responses containing CHRI be disseminated other than as governed by this Outsourcing Standard or more stringent contract requirements.

#### 6.0 *Personnel Security*

- 6.01 If a local, state, or federal written standard requires or authorizes a criminal history record check of the Authorized Recipient's personnel with access to

CHRI, then a criminal history record check shall be required of the Contractor's (and approved Sub-Contractor's) employees having access to CHRI. Criminal history record checks of Contractor and approved Sub-Contractor employees, at a minimum, will be no less stringent than criminal history record checks that are performed on the Authorized Recipient's personnel performing similar functions. Criminal history record checks must be completed prior to accessing CHRI under the contract.

- 6.02 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm in writing that each employee has certified in writing that he/she understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities. The Contractor shall maintain the employee certifications in a file that is subject to review during audits. Employees shall make such certification prior to performing work under the contract.
- 6.03 The Contractor shall maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur, and if a criminal history record check is required, maintain a list of personnel who have successfully completed criminal history record checks. The Contractor shall notify Authorized Recipients within 24 hours when additions or deletions occur.

## 7.0 *System Security*

- 7.01 The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy.
  - a. If CHRI can be accessed by unauthorized personnel via Wide Area Network/Local Area Network or the Internet, then the Contractor shall protect the CHRI with firewall-type devices to prevent such unauthorized access. These devices shall implement a minimum firewall profile as specified by the CJIS Security Policy in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.
  - b. Data encryption shall be required throughout the network passing CHRI through a shared public carrier network.
- 7.02 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.
  - a. CHRI shall be stored in a physically secure location.
  - b. The Authorized Recipient shall ensure that a procedure is in place for

sanitizing all fixed storage media (e.g., disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal, or reuse. Sanitization procedures include overwriting the media and/or degaussing the media.

- c. The Authorized Recipient shall ensure that a procedure is in place for the disposal or return of all non-fixed storage media (e.g., hard copies, print-outs).
- 7.03 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient, Contractor, or sub-Contractor must be assigned a unique identifying number.

## 8.0 *Security Violations*

### 8.01 Duties of the Authorized Recipient and Contractor

- a. The Contractor shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference.
- b. Pending investigation, the Contractor shall, upon detection or awareness, suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.
- c. The Contractor shall immediately (within four hours) notify the Authorized Recipient of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. Within five calendar days of such notification, the Contractor shall provide the Authorized Recipient a written report documenting such security violation, any corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.
- d. The Authorized Recipient shall immediately (within four hours) notify the State Compact Officer/Chief Administrator and the FBI Compact Officer of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator, if applicable, and the FBI Compact Officer, within five calendar days of receipt of the written report from the Contractor. The written report must include any corrective actions taken by the Contractor and the Authorized Recipient to resolve such security violation.

- 8.02 Termination of the contract by the Authorized Recipient for security violations
- a. The contract is subject to termination by the Authorized Recipient for security violations involving CHRI obtained pursuant to the contract.
  - b. The contract is subject to termination by the Authorized Recipient for the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.
  - c. If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient shall terminate the contract.
- 8.03 Suspension or termination of the exchange of CHRI for security violations
- a. Notwithstanding the actions taken by the State Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Compact Council or the United States Attorney General may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 CFR §906.2(d).
  - b. If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United States Attorney General by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be deleted or returned in accordance with the provisions and time frame as specified by the Authorized Recipient.
- 8.04 The Authorized Recipient shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following:
- a. The termination of a contract for security violations.
  - b. Security violations involving the unauthorized access to CHRI.
  - c. The Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.
- 8.05 The Compact Officer/Chief Administrator, Compact Council and the United States Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.
- 8.06 The Compact Officer/Chief Administrator, Compact Council, and the United

States Attorney General reserve the right to audit the Authorized Recipient and the Contractor's operations and procedures at scheduled or unscheduled times. The Compact Council, the United States Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the contract.

9.0 *Miscellaneous Provisions*

- 9.01 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, Compact Officer/Chief Administrator (where applicable), and the FBI.
- 9.02 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) The CJIS Security Policy.
- 9.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and the CHRI accessed therefrom and it is understood that there may be terms and conditions of the appended contract which impose more stringent requirements upon the Contractor.<sup>5</sup>
- 9.04. The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. Conformance to such security measures may not be less stringent than stated in this Outsourcing Standard without the consent of the Compact Council in consultation with the United States Attorney General.
- 9.05 This Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.
- 9.06 Appropriate notices, assurances, and correspondence to the FBI Compact Officer, Compact Council, and the United States Attorney General required by Section 8.0 of this Outsourcing Standard shall be forwarded by First Class Mail to:

FBI Compact Officer  
1000 Custer Hollow Road  
Module D-3  
Clarksburg, WV 26306

10.0 *Exemption from Above Provisions*

---

<sup>5</sup>Such conditions could include additional audits, fees, or security requirements. The Compact Council, Authorized Recipients, and the Compact Officer/Chief Administrator have the explicit authority to require more stringent standards than those contained in the Outsourcing Standard.

- 10.01 An Information Technology (IT) contract need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:
1. Access to CHRI by the IT contractor's personnel is limited solely for the development and/or maintenance of the Authorized Recipient's computer system;
  2. Access to CHRI is incidental, but necessary, to the duties being performed by the IT contractor;
  3. The computer system resides within the Authorized Recipient's facility;
  4. The Authorized Recipient's personnel supervise or work directly with the IT contractor personnel;
  5. The Authorized Recipient maintains complete, positive control of the IT contractor's access to the computer system and CHRI contained therein; and
  6. The Authorized Recipient retains all of the duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard.

10.02 An Authorized Recipient's contract where access to CHRI is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 4.0, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:

1. Access to CHRI by the Contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient;
2. Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor;

3. The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the Authorized Recipient;
4. The Contractor's personnel are subject to the same criminal history record checks as the Authorized Recipient's personnel;
5. The criminal history record checks of the Contractor personnel are completed prior to work on the contract or agreement;
6. The Authorized Recipient retains all other duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard; and
7. The Contractor stores the CHRI in a physically secure location.

**WSP Contract No. C130757GSC  
Amendment 1**

**WASHINGTON STATE PATROL  
CONTRACT AMENDMENT**

The above referenced Contract between the Washington State Patrol and the Quileute Housing Authority is hereby amended as follows:


- The end date shall be extended through September 19, 2021.
- EXHIBIT B CJIS Security Policy 5.1 shall be replaced with EXHIBIT B CJIS Security Policy 5.5.

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

QUILEUTE HOUSING AUTHORITY



---

FOR: John R. Batiste, Chief



---

Signature

6/8/18

---

Date

6/5/18

---

Date



**MEMORANDUM OF UNDERSTANDING**

**Between the**

**WASHINGTON STATE PATROL**

**And the**

**SUNNYSIDE HOUSING AUTHORITY**

**I. PURPOSE**

The parties to this Memorandum of Understanding (MOU) are the Washington State Patrol, Identification and Criminal History Section (WSP) and the Sunnyside Housing Authority, a non criminal justice agency (NCJA). This MOU sets forth the policy to ensure the protection of criminal history record information (CHRI) between the WSP, the NCJA, and the Federal Bureau of Investigation (FBI). This MOU provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CHRI data. This policy applies to the NCJA and its contractors with access to, or who operate in support of, non-criminal justice services and information.

**II. ADMINISTRATIVE RESPONSIBILITIES**

As participants in this MOU, the parties will develop mutually and separately appropriate procedures for transmission, dissemination, storage, and destruction of CHRI data.

- a. The Washington State Patrol. WSP shall ensure the NCJA complies with the Criminal Justice Information Services (CJIS) Security Policy (See Exhibit B) which includes authorized use of CHRI, dissemination of CHRI, statute authorization for civil applicant background checks conducted by noncriminal justice agencies, applicant notification and record challenge, security of CHRI, storage of CHRI, outsourcing of noncriminal justice administrative functions, and user fees. WSP will conduct regional audits of all agencies working under this MOU to ensure compliance to all state and federal standards.
- b. NCJA. The NCJA shall be responsible for ensuring:
  1. NCJA responds to requests for information by the FBI CJIS Division or the WSP in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of the agency.
  2. NCJA has formalized written procedures for the following, if applicable: criminal history use and dissemination, misuse, background checks, password management, storage, and destruction of CHRI.
  3. CHRI received as a result of licensing or employment purposes, pursuant to Public Law 92-544 is solely used for the purpose for which the record was requested. Subject fingerprints shall be submitted with all requests for CHRI for noncriminal justice purposes. Access to the FBI CJIS using name-based inquiry and record request messages is not permitted for noncriminal justice purpose, unless otherwise approved by the FBI.
  4. Access to CHRI by authorized officials is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or other authorized entities.

5. All fingerprint based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.
6. NCJA must notify the applicants fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The officials making the determination of suitability for licensing or employment shall provide the applicants the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record. These officials also must advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in Title 28, C.F.R. 16.34. Official making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so.
7. Appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity.
8. NCJA shall seek WSP permission prior to outsourcing noncriminal justice functions.
9. Outsourcing of noncriminal justice administrative functions requiring access to CHRI to either another governmental agency or a private contractor acting as an agent for the authorized receiving agency complies with the security and management control outsourcing standard for non-channelers (see Exhibit A).
10. NCJA is responsible for compliance to technical standards set forth by WSP and the CJIS Security Policy.
11. NCJA will conduct periodic self audits to ensure compliance with CJIS Security Policy.
12. NCJA will participate in WSP and FBI audits, provide plans for any compliance issues, and follow through to resolution within identified timeframes.
13. NCJA will ensure all appropriate staff members are trained according to the state and federal requirements.

### **III. CRIMINAL HISTORY RECORD INFORMATION RESPONSIBILITIES**

NCJA shall conform to system policies, as established by the FBI CJIS Division and WSP, before access to CHRI is permitted. This will allow for control over the data and give assurance of system security.

1. The rules and procedures governing access to CHRI shall apply equally to all participants in the system.
2. All noncriminal justice agencies with access to CHRI data must designate a specific unit, position, or personnel to access CHRI; noncriminal justice agencies must advise WSP of such personnel and changes to such designation.
3. All noncriminal justice agencies with access to CHRI data from the system shall permit an FBI CJIS Division or WSP audit team to conduct appropriate audits. NCJA must cooperate with these audits and respond promptly.

### **IV. SECURITY RESPONSIBILITIES**

#### **Technical Roles and Responsibilities**

NCJA must comply with and enforce system security. NCJA must have someone designated as the security point of contact (POC). Security POC's shall be responsible for the following:

1. Identifying the user of the hardware/software and ensuring that no unauthorized users have access to the same.
2. Identifying and documenting how the equipment is connected to the state system.

3. Ensuring that personnel security screening procedures are being followed as stated in the CJIS Security Policy.
4. Ensuring that appropriate hardware security measures are in place.
5. Supporting policy compliance and keeping the WSP informed of security incidents.
6. If the technical POC changes at your agency, notify WSP immediately.

#### **Security Enforcement**

NCJA is responsible for enforcing system security standards for their agency, in addition to all of the other agencies to which the NCJA provides CHRI information. Authorized users shall access and disseminate the CHRI data only for the purpose for which they are authorized. NCJA shall have a written policy for the discipline of policy violators.

#### **Technical Security Training**

All Information Technology (IT) employees who have access to and those who have direct responsibility to configure and maintain FBI CJIS systems must review security awareness training within six months of their appointment or assignment. Documentation pertaining to the materials used and those employees which receive security awareness training shall be maintained in a current status.

#### **Physical Security**

A physically secured location in a noncriminal justice facility, an area, a room, a group of rooms, that is/are subject to criminal justice agency management control security addendum and which contain hardware, software, and/or firmware (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch panels, etc.) that provide access to the CJIS sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that restrict unauthorized access.

All personnel with access to computer centers, CHRI, or areas where CHRI information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check. All personnel must review security awareness training within six months of their appointment or assignment.

#### **Personnel Security**

To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days of initial employment or assignment for all personnel who have authorized access to FBI CJIS information and those who have direct responsibility to configure and maintain computer systems and networks with access to FBI CJIS information. All requests from system access shall be made as specified by the CJIS Systems Officer (i.e. WSP Identification and Criminal History Section).

- c. NCJA shall use the data supplied by WSP and the FBI under this MOU only for the authorized purpose intended. NCJA shall not use this data for any other purpose and shall not disseminate this data with any other parties unless required by law. NCJA shall share any public disclosure requests regarding this data with the WSP.

#### **Storage**

Please see 'Security and Management Control Outsourcing Standard for Non-Channelers' (Exhibit A).

**V. LIAISON REPRESENTATIVES**

**For the Washington State Patrol:**

Jim Anderson, Administrator  
Criminal Records Division  
PO Box 42619  
Olympia WA 98504-2619  
Phone: (360) 534-2101  
Fax: (360) 534-2070  
E-mail: [jim.anderson@wsp.wa.gov](mailto:jim.anderson@wsp.wa.gov)

**For the Sunnyside Housing Authority:**

Ketha Kimbrough  
204 South 13th St  
Sunnyside WA 98944  
509-837-5061  
[ketha@sunnysideha.org](mailto:ketha@sunnysideha.org)

**VI. INDEMNIFICATION**

Each party shall defend, protect and hold harmless the other party from and against all claims, suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing this MOU.

**VII. PERIOD OF MOU**

This MOU becomes effective on the date of the last signature and continues for three years and may be renewed. It may be modified by mutual written consent of the two agencies. Liaison Representatives may modify Exhibit A by mutual written consent of the two agencies without changing the general conditions of this MOU.

**VIII. TERMINATION**

Except as otherwise provided in this MOU, either party may terminate this MOU upon ninety (90) days' written notification to the other party. If this MOU is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this MOU for performance prior to the effective date of termination.

**IX. DISPUTES**

In the event that a dispute arises under this MOU, it shall be determined in the following manner: The Chief of WSP, or designee, shall appoint one member to the Dispute Board. NCJA shall appoint one member to the Dispute Board. The Chief of WSP, or designee, and the NCJA shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. If applicable and as an alternative to this process, either of the parties may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.

**X. EXHIBITS**

The exhibits listed below are incorporated into and made a part of this MOU:

Exhibit A - 'Security and Management Control Outsourcing Standard for Non-Channelers'

Exhibit B - Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.2, published 8/9/2013 which is available at the following link: [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center). WSP will provide a copy of the manual upon request.

**XI. ORDER OF PRECEDENCE**

In the event of any inconsistency in the terms of this MOU, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

- a. Applicable federal and state statutes and regulations;
- b. The Terms and Conditions contained in this MOU;
- c. The Exhibits attached to this MOU;
- d. Any other provisions of the MOU, whether incorporated by reference or otherwise.

**XII. ALL WRITINGS CONTAINED HEREIN**

This MOU contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this MOU shall be deemed to exist or to bind any of the parties hereto.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL

  
\_\_\_\_\_  
John R. Batiste, Chief

\_\_\_\_\_  
Date 9/20/13

SUNNYSIDE HOUSING AUTHORITY

  
\_\_\_\_\_  
Ketha Kimbrough, Executive Director

\_\_\_\_\_  
Date September 19, 2013

## SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD for NON-CHANNELERS

The goal of this document is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the Contractor. Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security and Management Control Outsourcing Standard (Outsourcing Standard) is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI without a direct connection to the FBI CJIS Wide Area Network (WAN).

### 1.0 *Definitions*

- 1.01 *Access to CHRI* means to view or make use of CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by title 42, United States Code, section 14614(b).
- 1.02 *Authorized Recipient* means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.
- 1.03 *Chief Administrator* means the primary administrator of a Nonparty State’s criminal history record repository or a designee of such administrator who is

a regular full-time employee of the repository, which is also referred to as the State Identification Bureau (SIB) Chief.

- 1.04 *CHRI*, as referred to in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.
- 1.05 *Criminal History Record Check*, for purposes of this Outsourcing Standard only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.
- 1.06 *Compact Officer*, as provided in Article I(2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the compact among federal agencies], or (B) with respect to a Party State, the chief administrator of the State's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.
- 1.07 *Contractor* means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI.
- 1.08 *Dissemination* means the disclosure of CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 1.09 *Noncriminal Justice Administrative Functions* means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:
1. Making fitness determinations/recommendations
  2. Obtaining missing dispositions
  3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General
  4. Other authorized activities relating to the general handling, use, and storage of CHRI

- 1.10 *Noncriminal Justice Purposes*, as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.
- 1.11 *Outsourcing Standard* means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. This Outsourcing Standard authorizes access to CHRI for noncriminal justice purposes, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.
- 1.12 *Physically Secure Location* means a facility or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CHRI and associated information systems.
- 1.13 *Positive Identification*, as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints<sup>1</sup> or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other non-unique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.
- 1.14 *Public Carrier Network* means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: Dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.
- 1.15 *Security Violation* means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in

---

<sup>1</sup> The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning positive identification may be obtained from the FBI Compact Council office.



violation of: (A) Federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

2.0 *Responsibilities of the Authorized Recipient*

- 2.01 Prior to engaging in outsourcing any noncriminal justice administrative functions, the Authorized Recipient shall: (a) Request and receive written permission from (1) the State Compact Officer/Chief Administrator<sup>2</sup> or (2) the FBI Compact Officer<sup>3</sup>; (b) provide the Compact Officer/Chief Administrator copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested; and (c) inquire of the FBI Compact Officer whether a prospective Contractor has any security violations (See Section 8.04). The FBI Compact Officer will report those findings to the Authorized Recipient and, when applicable, to the State Compact Officer/Chief Administrator.
- 2.02 The Authorized Recipient shall execute a contract or agreement prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.
- 2.03 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; limit retention of the information to a period of time not to exceed that period of time the Authorized Recipient is permitted to retain such information; prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General; ensure the security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; and ensure that Contractor

---

<sup>2</sup>The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and Authorized Recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.

<sup>3</sup>State or local Authorized Recipients based on State or Federal Statutes shall contact the State Compact Officer/Chief Administrator. Federal or Regulatory Agency Authorized Recipients shall contact the FBI Compact Officer.

personnel comply with this Outsourcing Standard.

- a. The Authorized Recipient shall conduct criminal history record checks of Contractor personnel having access to CHRI if such checks are required or authorized of the Authorized Recipient's personnel having similar access.<sup>4</sup> The Authorized Recipient shall maintain updated records of Contractor personnel who have access to CHRI and update those records within 24 hours when changes to that access occur and, if a criminal history record check is required, the Authorized Recipient shall maintain a list of Contractor personnel who successfully completed the criminal history record check.
- b. The Authorized Recipient shall ensure that the Contractor maintains site security.
- c. The Authorized Recipient shall ensure that the most current version of both the Outsourcing Standard and the CJIS Security Policy are incorporated by reference at the time of contract, contract renewal, or within 30 calendar days (unless otherwise directed) of notification of successor versions of the Outsourcing Standard and/or CJIS Security Policy, whichever is sooner. The Authorized Recipient shall notify the Contractor within 30 calendar days (unless otherwise directed) of FBI notification regarding changes or updates to the Outsourcing Standard and/or CJIS Security Policy.

- 2.04 The Authorized Recipient shall understand the communications and record capabilities of the Contractor which has access to federal or state records through, or because of, its outsourcing relationship with the Authorized Recipient. The Authorized Recipient shall maintain an updated topological drawing which depicts the interconnectivity of the Contractor's network configuration.
- 2.05 The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the Outsourcing Standard. The Authorized Recipient shall certify to the Compact Officer/Chief Administrator that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.

---

<sup>4</sup>If a national criminal history record check of Authorized Recipient personnel having access to CHRI is mandated or authorized by a federal statute, executive order, or state statute approved by the Attorney General under Public Law 92-544, the State Compact Officer/Chief Administrator and/or the FBI Compact Officer must ensure Contractor personnel having similar access are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives. The national criminal history record checks of Contractor personnel with access to CHRI cannot be outsourced and must be performed by the Authorized Recipient.

2.06 The Authorized Recipient shall provide written notice of any early voluntary termination of the contract to the Compact Officer/Chief Administrator or the FBI Compact Officer.

3.0 *Responsibilities of the Contractor*

3.01 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the CJIS Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

3.02 The Contractor shall develop, document, administer, and maintain a Security Program (Physical, Personnel, and Information Technology) to comply with the most current Outsourcing Standard and the most current FBI *CJIS Security Policy*. The Security Program shall describe the implementation of the security requirements described in this Outsourcing Standard and the FBI *CJIS Security Policy*. In addition, the Contractor is also responsible to set, maintain, and enforce the standards for the selection, supervision, and separation of personnel who have access to CHRI. The Authorized Recipient shall provide the written approval of a Contractor's Security Program.

3.03 The requirements for a Security Program should include, at a minimum:

- a) Description of the implementation of the security requirements described in this Outsourcing Standard and the *CJIS Security Policy*.
- b) Security Training.
- c) Guidelines for documentation of security violations.
- d) Standards for the selection, supervision, and separation of personnel with access to CHRI.

\*\*If the Contractor is using a corporate policy, it must meet the requirements outlined in this Outsourcing Standard and the *CJIS Security Policy*. If the corporate policy is not this specific, it must flow down to a level where the documentation supports these requirements.

3.04 Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. The Authorized Recipient shall review and provide to the Contractor written approval of the Security Training Program. Training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall annually, not later than the anniversary date of the contract, certify in writing to the Authorized Recipient that annual refresher training was completed for those Contractor personnel with access

to CHRI.

- 3.05 The Contractor shall make its facilities available for announced and unannounced audits performed by the Authorized Recipient, the state, or the FBI on behalf of the Compact Council.
- 3.06 The Contractor's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI CJIS Division. During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.
- 3.07 The Contractor shall maintain CHRI only for the period of time necessary to fulfill its contractual obligations but not to exceed the period of time that the Authorized Recipient is authorized to maintain and does maintain the CHRI.
- 3.08 The Contractor shall maintain a log of any dissemination of CHRI, for a minimum of 365 days.

#### 4.0 *Site Security*

- 4.01 The Authorized Recipient shall ensure that the Contractor site(s) is a physically secure location to protect against any unauthorized access to CHRI.

#### 5.0 *Dissemination*

- 5.01 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 5.02 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) The Authorized Recipient and the secondary recipient with unique identifiers, (B) the record disseminated, (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.
- 5.03 If CHRI is stored or disseminated in an electronic format, the Contractor shall protect against unauthorized access to the equipment and any of the data. In no event shall responses containing CHRI be disseminated other than as governed by this Outsourcing Standard or more stringent contract requirements.

#### 6.0 *Personnel Security*

- 6.01 If a local, state, or federal written standard requires or authorizes a criminal history record check of the Authorized Recipient's personnel with access to

CHRI, then a criminal history record check shall be required of the Contractor's (and approved Sub-Contractor's) employees having access to CHRI. Criminal history record checks of Contractor and approved Sub-Contractor employees, at a minimum, will be no less stringent than criminal history record checks that are performed on the Authorized Recipient's personnel performing similar functions. Criminal history record checks must be completed prior to accessing CHRI under the contract.

- 6.02 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm in writing that each employee has certified in writing that he/she understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities. The Contractor shall maintain the employee certifications in a file that is subject to review during audits. Employees shall make such certification prior to performing work under the contract.
- 6.03 The Contractor shall maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur, and if a criminal history record check is required, maintain a list of personnel who have successfully completed criminal history record checks. The Contractor shall notify Authorized Recipients within 24 hours when additions or deletions occur.

## 7.0 *System Security*

- 7.01 The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy.
  - a. If CHRI can be accessed by unauthorized personnel via Wide Area Network/Local Area Network or the Internet, then the Contractor shall protect the CHRI with firewall-type devices to prevent such unauthorized access. These devices shall implement a minimum firewall profile as specified by the CJIS Security Policy in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.
  - b. Data encryption shall be required throughout the network passing CHRI through a shared public carrier network.
- 7.02 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.
  - a. CHRI shall be stored in a physically secure location.
  - b. The Authorized Recipient shall ensure that a procedure is in place for

sanitizing all fixed storage media (e.g., disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal, or reuse. Sanitization procedures include overwriting the media and/or degaussing the media.

- c. The Authorized Recipient shall ensure that a procedure is in place for the disposal or return of all non-fixed storage media (e.g., hard copies, print-outs).
- 7.03 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient, Contractor, or sub-Contractor must be assigned a unique identifying number.

## 8.0 *Security Violations*

### 8.01 Duties of the Authorized Recipient and Contractor

- a. The Contractor shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference.
- b. Pending investigation, the Contractor shall, upon detection or awareness, suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.
- c. The Contractor shall immediately (within four hours) notify the Authorized Recipient of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. Within five calendar days of such notification, the Contractor shall provide the Authorized Recipient a written report documenting such security violation, any corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.
- d. The Authorized Recipient shall immediately (within four hours) notify the State Compact Officer/Chief Administrator and the FBI Compact Officer of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator, if applicable, and the FBI Compact Officer, within five calendar days of receipt of the written report from the Contractor. The written report must include any corrective actions taken by the Contractor and the Authorized Recipient to resolve such security violation.

- 8.02 Termination of the contract by the Authorized Recipient for security violations
- a. The contract is subject to termination by the Authorized Recipient for security violations involving CHRI obtained pursuant to the contract.
  - b. The contract is subject to termination by the Authorized Recipient for the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.
  - c. If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient shall terminate the contract.
- 8.03 Suspension or termination of the exchange of CHRI for security violations
- a. Notwithstanding the actions taken by the State Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Compact Council or the United States Attorney General may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 CFR §906.2(d).
  - b. If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United States Attorney General by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be deleted or returned in accordance with the provisions and time frame as specified by the Authorized Recipient.
- 8.04 The Authorized Recipient shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following:
- a. The termination of a contract for security violations.
  - b. Security violations involving the unauthorized access to CHRI.
  - c. The Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.
- 8.05 The Compact Officer/Chief Administrator, Compact Council and the United States Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.
- 8.06 The Compact Officer/Chief Administrator, Compact Council, and the United

States Attorney General reserve the right to audit the Authorized Recipient and the Contractor's operations and procedures at scheduled or unscheduled times. The Compact Council, the United States Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the contract.

#### 9.0 *Miscellaneous Provisions*

- 9.01 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, Compact Officer/Chief Administrator (where applicable), and the FBI.
- 9.02 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) The CJIS Security Policy.
- 9.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and the CHRI accessed therefrom and it is understood that there may be terms and conditions of the appended contract which impose more stringent requirements upon the Contractor.<sup>5</sup>
- 9.04 The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. Conformance to such security measures may not be less stringent than stated in this Outsourcing Standard without the consent of the Compact Council in consultation with the United States Attorney General.
- 9.05 This Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.
- 9.06 Appropriate notices, assurances, and correspondence to the FBI Compact Officer, Compact Council, and the United States Attorney General required by Section 8.0 of this Outsourcing Standard shall be forwarded by First Class Mail to:

FBI Compact Officer  
1000 Custer Hollow Road  
Module D-3  
Clarksburg, WV 26306

#### 10.0 *Exemption from Above Provisions*

---

<sup>5</sup>Such conditions could include additional audits, fees, or security requirements. The Compact Council, Authorized Recipients, and the Compact Officer/Chief Administrator have the explicit authority to require more stringent standards than those contained in the Outsourcing Standard.



- 10.01 An Information Technology (IT) contract need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:
1. Access to CHRI by the IT contractor's personnel is limited solely for the development and/or maintenance of the Authorized Recipient's computer system;
  2. Access to CHRI is incidental, but necessary, to the duties being performed by the IT contractor;
  3. The computer system resides within the Authorized Recipient's facility;
  4. The Authorized Recipient's personnel supervise or work directly with the IT contractor personnel;
  5. The Authorized Recipient maintains complete, positive control of the IT contractor's access to the computer system and CHRI contained therein; and
  6. The Authorized Recipient retains all of the duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard.

10.02 An Authorized Recipient's contract where access to CHRI is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 4.0, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:

1. Access to CHRI by the Contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient;
2. Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor;

3. The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the Authorized Recipient;
4. The Contractor's personnel are subject to the same criminal history record checks as the Authorized Recipient's personnel;
5. The criminal history record checks of the Contractor personnel are completed prior to work on the contract or agreement;
6. The Authorized Recipient retains all other duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard; and
7. The Contractor stores the CHRI in a physically secure location.

WASHINGTON STATE PATROL  
CONTRACT AMENDMENT

The above referenced Contract between the Washington State Patrol and the Sunnyside Housing Authority is hereby amended as follows:

- The end date shall be extended through September 25, 2021.
- EXHIBIT B CJIS Security Policy 5.1 shall be replaced with EXHIBIT B CJIS Security Policy 5.5.

All other terms and conditions of this Contract remain in full force and effect.

THIS AMENDMENT is executed by the persons signing below, who warrant that they have the authority to execute this Amendment.

STATE OF WASHINGTON  
WASHINGTON STATE PATROL



FOR: John R. Batiste, Chief

3/24/2017

Date

SUNNYSIDE HOUSING AUTHORITY



Signature

March 21, 2017

Date