52.212-4 Contract Terms and Conditions - Commercial Items. (Oct 2018)

52.212-5 -- Contract Terms and Conditions Required to Implement Statutes or Executive Orders -- Commercial Items (Jan 2021) (Deviation Apr 2020)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(2) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).

(3) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Aug 2020) (Section 889(a)(1)(A) of Pub. L. 115-232).

(4) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015)

(5) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).

(6) 52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004) (Public Laws 108-77, 108-78 (19 U.S.C. 3805 note)).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the contracting officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

[Contracting Officer check as appropriate.]

X (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Jun 2020), with Alternate I (Oct 1995) (41 U.S.C. 4704 and 10 U.S.C. 2402).

X (2) 52.203-13, Contractor Code of Business Ethics and Conduct (Jun 2020) (41 U.S.C. 3509).

_ (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (Jun 2010) (Section 1553 of Pub L. 111-5) (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009).

X (4) 52.204-10, Reporting Executive compensation and First-Tier Subcontract Awards (Jun 2020) (Pub. L. 109-282) (31 U.S.C. 6101 note).

_ (5) [Reserved]

X (6) 52.204-14, Service Contract Reporting Requirements (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

_ (7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

X (8) 52.209-6, Protecting the Government' Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (Jun 2020) (31 U.S.C. 6101 note).

X (9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Oct 2018) (41 U.S.C. 2313).

_ (10) [Reserved]

_ (11)(i) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (Mar 2020) (15 U.S.C. 657a).

_ (ii) Alternate I (Mar 2020) of 52.219-3.

_ (12) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Mar 2020) (if the offeror elects to waive the preference, it shall so indicate in its offer)(15 U.S.C. 657a).

_ (ii) Alternate I (Mar 2020) of 52.219-4.

_ (13) [Reserved]

_ (14) (i) 52.219-6, Notice of Total Small Business Aside (Nov 2020) (15 U.S.C. 644).

_ (ii) Alternate I (Mar 2020) of 52.219-6.

_ (15) (i) 52.219-7, Notice of Partial Small Business Set-Aside (Nov 2020) (15 U.S.C. 644).

_ (ii) Alternate I (Mar 2020) of 52.219-7.

X (16) 52.219-8, Utilization of Small Business Concerns (Oct 2018) (15 U.S.C. 637(d)(2) and (3)).

X (17) (i) 52.219-9, Small Business Subcontracting Plan (Jun 2020) (15 U.S.C. 637 (d)(4))

_ (ii) Alternate I (Nov 2016) of 52.219-9.

X (iii) Alternate II (Nov 2016) of 52.219-9.

_ (iv) Alternate III (Jun 2020) of 52.219-9.

_ (v) Alternate IV (June 2020) of 52.219-9.

_ (18)(i) 52.219-13, Notice of Set-Aside of Orders (Mar 2020) (15 U.S.C. 644(r)).

_(ii) Alternate I (Mar 2020) of 52.219-13

_ (19) 52.219-14, Limitations on Subcontracting (Mar 2020) (15 U.S.C. 637(a)(14)).

X (20) 52.219-16, Liquidated Damages—Subcontracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).

_ (21) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (Mar 2020) (15 U.S.C. 657f).

X (22)(i) 52.219-28, Post Award Small Business Program Rerepresentation (Nov 2020) (15 U.S.C. 632(a)(2)).

_(ii) Alternate I (Mar 2020) of 52.219-28

_ (23) 52.219-29, Notice of Set-Aside for, or Sole Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (Mar 2020) (15 U.S.C. 637(m)).

_ (24) 52.219-30, Notice of Set-Aside for, or Sole Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (Mar 2020) (15 U.S.C. 637(m)).

_ (25) 52.219-32, Orders Issued Directly Under Small Business Reserves (Mar 2020) (15 U.S.C. 644(r)).

_ (26) 52.219-33, Nonmanufacturer Rule (Mar 2020) (15 U.S.C. 637(a)(17)).

X (27) 52.222-3, Convict Labor (June 2003) (E.O. 11755).

X (28) 52.222-19, Child Labor—Cooperation with Authorities and Remedies (Jan 2020) (E.O. 13126).

X (29) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

X (30)(i) 52.222-26, Equal Opportunity (Sep 2016) (E.O. 11246).

_ (ii) Alternate I (Feb 1999) of 52.222-26

X (31) 52.222-35, Equal Opportunity for Veterans (Jun 2020) (38 U.S.C. 4212).

_ (ii) Alternate I (July 2014) of 52.222-35

X (32) 52.222-36, Equal Opportunity for Workers with Disabilities (Jun 2020) (29 U.S.C. 793).

_ Alternate I (July 2014) of 52.222-36

X (33) 52.222-37, Employment Reports on Veterans (Jun 2020) (38 U.S.C. 4212).

X (34) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).

X (35) (i) 52.222-50, Combating Trafficking in Persons (Oct 2020) (22 U.S.C. chapter 78 and E.O. 13627).

_ (ii) Alternate I (Mar 2015) of 52.222-50, (22 U.S.C. chapter 78 and E.O. 13627).

_ (36) 52.222-54, Employment Eligibility Verification (Oct 2015). (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)

_ (37)(i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008) (42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

_ (ii) Alternate I (May 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

_ (38) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (Jun 2016) (E.O.13693).

_ (39) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (Jun 2016) (E.O. 13693).

_ (40) (i) 52.223-13, Acquisition of EPEAT® -Registered Imaging Equipment (Jun 2014) (E.O.s 13423 and 13514).

_ (ii) Alternate I (Oct 2015) of 52.223-13.

_ (41) (i) 52.223-14, Acquisition of EPEAT® -Registered Television (Jun 2014) (E.O.s 13423 and 13514).

_ (ii) Alternate I (Jun 2014) of 52.223-14.

_(42) 52.223-15, Energy Efficiency in Energy-Consuming Products (May 2020) (42 U.S.C. 8259b).

_ (43) 52.223-16, Acquisition of EPEAT® -Registered Personal Computer Products (Oct 2015) (E.O.s 13423 and 13514)

_ (ii) Alternate I (Jun 2014) of 52.223-16.

X (44) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging while Driving (Jun 2020) (E.O. 13513).

_ (45) 52.223.20, Aerosols (Jun 2016) (E.O. 13693).

_ (46) 52.223.21, Foams (Jun 2016) (E.O. 13696).

X (47) (i) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).

X (ii) Alternate I (Jan 2017) of 52.224-3.

_ (48) 52.225-1, Buy American Act--Supplies (Jan 2021) (41 U.S.C. chapter 83).

_ (49) (i) 52.225-3, Buy American Act--Free Trade Agreements--Israeli Trade Act (Jan 2021) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43).

_ (ii) Alternate I (May 2014) of 52.225-3.

_ (iii) Alternate II (May 2014) of 52.225-3.

_ (iv) Alternate III (May 2014) of 52.225-3.

_ (50) 52.225-5, Trade Agreements (Oct 2019) (19 U.S.C. 2501, *et seq.*, 19 U.S.C. 3301 note).

X (51) 52.225-13, Restrictions on Certain Foreign Purchases (Jun 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

_ (52) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2303 Note).

_ (53) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).

_ (54) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).

_ (55) 52.229-12, Tax on Certain Foreign Procurements (Jun 2020)

_ (56) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).

_ (57) 52.232-30, Installment Payments for Commercial Items (Jan 2017) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).

X (58) 52.232-33, Payment by Electronic Funds Transfer— System for Award Management (Oct 2018) (31 U.S.C. 3332).

_ (59) 52.232-34, Payment by Electronic Funds Transfer— Other Than System for Award Management (Jul 2013) (31 U.S.C. 3332).

_ (60) 52.232-36, Payment by Third Party (May 2014) (31 U.S.C. 3332).

X (61) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).

X (62) 52.242-5, Payments to Small Business Subcontractors (Jan 2017) (15 U.S.C. 637(d)(12)).

_ (63) (i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631).

_ (ii) Alternate I (Apr 2003) of 52.247-64.

_ (iii) Alternate II (Feb 2006) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or executive orders applicable to acquisitions of commercial items:

[*Contracting Officer check as appropriate.*]

_ (1) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67.).

_ (2) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

_ (3) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards -- Price Adjustment (Multiple Year and Option Contracts) (Aug 2018) (29 U.S.C.206 and 41 U.S.C. chapter 67).

_ (4) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards -- Price Adjustment (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

_ (5) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (May 2014) (41 U.S.C. chapter 67).

_ (6) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67).

_ (7) 52.222-55, Minimum Wages Under Executive Order 13658 (Nov 2020)

_ (8) 52.222-62, Paid Sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).

_ (9) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (Jun 2020) (42 U.S.C. 1792).

(d) *Comptroller General Examination of Record* The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records -- Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e) (1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c) and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause—

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (Jun 2020) (41 U.S.C. 3509).

(ii) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(iii) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).

(iv) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Aug 2020) (Section 889(a)(1)(A) of Pub. L. 115-232).

(v) 52.219-8, Utilization of Small Business Concerns (Oct 2018) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $700,000 ($1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(vi) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

(vii) 52.222-26, Equal Opportunity (Sep 2015) (E.O. 11246).

(viii) 52.222-35, Equal Opportunity for Veterans (Jun 2020) (38 U.S.C. 4212).

(ix) 52.222-36, Equal Opportunity for Workers with Disabilities (Jun 2020) (29 U.S.C. 793).

(x) 52.222-37, Employment Reports on Veterans (Jun 2020) (38 U.S.C. 4212).

(xi) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(xii) 52.222-41, Service Contract Labor Standards (Aug 2018), (41 U.S.C. chapter 67).

(xiii) (A) 52.222-50, Combating Trafficking in Persons (Nov 2020) (22 U.S.C. chapter 78 and E.O. 13627).

(B) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 E.O. 13627).

(xiv) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (May 2014) (41 U.S.C. chapter 67.)

(xv) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67)

(xvi) 52.222-54, Employment Eligibility Verification (Oct 2015) (E. O. 12989).

(xvii) 52.222-55, Minimum Wages Under Executive Order 13658 (Nov 2020).

(xviii) 52.222-62, Paid sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).

(xix) (A) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).

(B) Alternate I (Jan 2017) of 52.224-3.

(xx) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

(xxi) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (Jun 2020) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xxii) 52.247-64, Preference for Privately-Owned U.S. Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64

(2) While not required, the contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of Clause)

Additional FAR Clauses incorporated by Reference:

52.204-13 System for Award Management Maintenance (Oct 2018)

FAR Clauses incorporated by Full Text:

52.203-17 Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights. (Jun 2020)

(a) This contract and employees working on this contract will be subject to the whistleblower rights and remedies in the pilot program on Contractor employee whistleblower protections established at 41 U.S.C. 4712 by section 828 of the National Defense Authorization Act for Fiscal Year 2013 (Pub. L. 112-239) and FAR 3.908.

(b) The Contractor shall inform its employees in writing, in the predominant language of the workforce, of employee whistleblower rights and protections under 41 U.S.C. 4712, as described in section FAR 3.908.

(c) The Contractor shall insert the substance of this clause, including this paragraph (c), in all subcontracts over the simplified acquisition threshold as defined in FAR 2.101 on the date of subcontract award.

(End of clause)

FAR 52.217-8 Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within one day prior to contract expiration.

(End of clause)

FAR 52.217-9 Option to Extend the Term of the Contract (Mar 2000)

(a)The Government may extend the term of this contract by written notice to the Contractor within *one day prior to contract expiration*; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least *30 calendar days* before the contract expires. The preliminary notice does not commit the Government to an extension.

(b)If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c)The total duration of this contract, including the exercise of any options under this clause, shall not exceed *five years, six months*.

(End of clause)

FAR Deviation Clauses incorporated by Full Text:

52.204-23 PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES (DEVIATION 2020-05) (APRIL 10, 2020)

(a) *Definitions*. As used in this clause—

"Covered article" means any hardware, software, or service that–

(1) Is developed or provided by a covered entity;

(2) Includes any hardware, software, or service developed or provided in whole or in part by a covered entity; or

(3) Contains components using any hardware or software developed in whole or in part by a covered entity.

"Covered entity" means–

(1) Kaspersky Lab;

(2) Any successor entity to Kaspersky Lab;

(3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or

(4) Any entity of which Kaspersky Lab has a majority ownership.

(b) *Prohibition*. Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits Government use of any covered article. The Contractor is prohibited from—

(1) Providing any covered article that the Government will use on or after October 1, 2018; and

(2) Using any covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the contract.

(c) *Reporting requirement*.

(1) In the event the Contractor identifies a covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or any other source, the Contractor shall report, in writing via email, to the Contracting Officer, Contracting Officer's Representative, and the Enterprise Security Operations Center (SOC) at (b)(7)(E) with required information contained in the body of the email. In the case of the Department of Defense, the Contractor shall report to the website at

(b)(7)(E) For indefinite delivery contracts, the Contractor shall report to the Enterprise SOC, Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) and Contracting Officer's Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided a(b)(7)(E)

(2) The Contractor shall report the following information pursuant to paragraph (c)(1) of this clause:

(i) Within 1 business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; brand; model number (Original Equipment Manufacturer (OEM) number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the report pursuant to paragraph (c)(1) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of a covered article, any reasons that led to the use or submission of the covered article, and any additional efforts that will be incorporated to prevent future use or submission of covered articles.

(d) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts, including subcontracts for the acquisition of commercial items.

(End of clause)

52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (DEVIATION 20-05) (DEC 2020)

(a) *Definitions.* As used in this clause—

"Backhaul" means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

"Covered foreign country" means The People's Republic of China.

"Covered telecommunications equipment or services" means–

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

"Critical technology" means–

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

"Interconnection arrangements" means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

"Reasonable inquiry" means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

"Roaming" means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

"Substantial or essential component" means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) *Prohibition.*

(1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115–232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115–232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) *Exceptions.* This clause does not prohibit contractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) *Reporting requirement.*

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause in writing via email to the Contracting Officer, Contracting Officer's Representative, and the Network Operations Security Center (NOSC) at (b)(7)(E) with required information in the body of the email. In the case of the Department of Defense, the

Contractor shall report to the website at (b)(7)(E) For indefinite delivery contracts, the Contractor shall report to the NOSC, Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) and Contracting Officer's Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at (b)(7)(E)

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

52.232-40 Providing Accelerated Payments to Small Business Subcontractors. (DEC 2013) (DEVIATION APR 2020)

(a)(1) In accordance with 31 U.S.C. 3903 and 10 U.S.C. 2307, upon receipt of accelerated payments from the Government, the Contractor shall make accelerated payments to its small business subcontractors under this contract in accordance with the accelerated payment date established, to the maximum extent practicable and prior to when such payment is otherwise required under the applicable contract or subcontract, with a goal of 15 days after receipt of a proper invoice and all other required documentation from the small business subcontractor if a specific payment date is not established by contract.

(2) The Contractor agrees to make such payments to its small business subcontractors without any further consideration from or fees charged to the subcontractor.

(b) The acceleration of payments under this clause does not provide any new rights under the Prompt Payment Act.

(c) Include the substance of this clause, including this paragraph (c), in all subcontracts with small business concerns, including subcontracts with small business concerns for the acquisition of commercial items.

(End of clause)

HSAR Clauses incorporated by Reference:

[*Contracting Officer check as appropriate.*]

X 3052.203-70, Instructions for Contractor Disclosure of Violations (Sep 2012)

X 3052.205-70, Advertisements, Publicizing Awards, and Releases (Sep 2012)

_3052.209-71, Reserve Officer Training Corps and Military Recruiting on Campus (Dec 2003)

X 3052.219-70 Small Business Subcontracting Plan Reporting (Jun 2006)

X 3052.219-71 DHS Mentor Protégé Program (Jun 2006)

X 3052.219-72 Evaluation of Prime Contractor Participation in DHS Mentor Protégé Program (Jun 2006)

X 3052.242-72 Contracting Officer's Technical Representative (Dec 2003)

HSAR Clauses in full text

HSAR 3052.204-71 Contractor Employee Access (Sep 2012)

(a) *Sensitive Information,* as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Pub. L. 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, part 1520, as amended, Policies and Procedures of Safeguarding and Control of SSI, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as For Official Use Only, which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated sensitive or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) Information Technology Resources include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(End of clause)

Alternate II **(JUN 2006)** When the Department has determined contract employee access to sensitive information or Government facilities must be limited to U.S. citizens and lawful permanent residents, but the contract will not require access to IT resources, add the following paragraphs:

(g) Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident Card (USCIS I-551). Any exceptions must be approved by the Department's Chief Security Officer or designee.

(h) Contractors shall identify in their proposals, the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the Contracting Officer.

(End of clause)

Special Clause Safeguarding of Sensitive Information (Mar 2015)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Definitions*. As used in this clause—

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107- 296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

"Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) *Authorities.* The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
(2) DHS Sensitive Systems Policy Directive 4300A
(3) DHS 4300A Sensitive Systems Handbook and Attachments
(4) DHS Security Authorization Process Guide
(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
(7) DHS Information Security Performance Plan (current fiscal year)
(8) DHS Privacy Incident Handling Guidance
(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html
(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

(d) *Handling of Sensitive Information.* Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA),* as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) *Authority to Operate*. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 9.1, July 24, 2012), or any successor publication, and the *Security Authorization Process Guide* including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) Independent Assessment. Contractors shall have an independent third party

validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods:
(1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) *Security Review.* The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to

coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Continuous Monitoring.* All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) Sensitive Information Incident Reporting Requirements.

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or

Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime contractor location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
(v) Contracting Officer POC (address, telephone, email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

(g) Sensitive Information Incident Response Requirements.

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and

Headquarters or Component Privacy Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(i) Inspections,
(ii) Investigations,
(iii) Forensic reviews, and
(iv) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(h) *Additional PII and/or SPII Notification Requirements*.

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the DHS Privacy Incident Handling Guidance. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;
(ii) A description of the types of PII and SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;
(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(i) *Credit Monitoring Requirements*. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*.

(End of Special Clause)

Special Clause Information Technology Security and Privacy Training (Mar 2015)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The

Contractor shall insert the substance of this clause in all subcontracts.

(b) *Security Training Requirements*.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

(c) *Privacy Training Requirements.* All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting Personal*

Information before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors.

Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e- mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(End of special clause)

Performance Work Statement (PWS)
Department of Homeland Security (DHS),
Immigration and Customs Enforcement (ICE)
Law Enforcement Investigative Database Subscription
March 5, 2021

1. BACKGROUND

The intent of this Performance Work Statement (PWS) is to procure a web-based law enforcement investigative database subscription service to assist Immigration, Customs and Enforcement (ICE) mission of conducting criminal investigations that protect the United States against terrorists and criminal organizations that threaten our safety and national security; to combat transnational criminal enterprises that see to exploit America's legitimate trade, travel and financial systems. ICE investigative agents require a robust analytical research tool for its in-depth exploration of persons of interest and vehicles.

The purpose of this contract is to provide ICE agents an investigative database system to further strategize arrests to minimize and, in some cases, avoid impact of potential injury. ICE requirement of a web-based law enforcement investigative database platform is to include, integration access to public records and commercial data with uninterrupted service, integrate investigative capabilities with the license plate recognition capabilities to be utilized by multiple ICE Directorates to include but not limited to Homeland Security Investigative (HSI), Enforcement and Removal Operations (ERO) and Office of Professional Responsibility (OPR). Use of this database subscription services furthers the criminal law enforcement mission.

1.1 **DHS/ICE**

ICE is the largest investigative agency in the Department of Homeland Security (DHS) and was formally established on March 1, 2003. ICE's primary mission is to protect national security, public safety, and the integrity of the US borders through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration.

ICE investigates a range of domestic and international activities including:

- Human smuggling and trafficking;
- Narcotics, cultural property, weapons and other contraband smuggling;
- Export enforcement, e.g., illegal arms and dual-use equipment;
- Financial crimes;
- Commercial fraud;
- Intellectual property rights violations;
- Cyber-crimes;
- Immigration fraud; and,
- Human rights violations.

The law enforcement investigative database system currently supports over 11,000 users across multiple program areas with analytical data and concrete information to search high risk and politically exposed criminal activity worldwide. The database subscription service plays a

crucial role in ICEs overall investigative mission success. Moreover, the agency can achieve cost savings to the government when reducing the work hours required for physical surveillance.

2.0 SCOPE/OBJECTIVES

The Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement (ICE) houses a large dataset of detailed data that is available to an assortment of approved law enforcement users. ICE criminal law enforcement mission; to enhance investigations to support all mission activities mentioned above in over 50 countries and 67 locations globally; to provide a platform where the continuity of public records and commercial data is available on an uninterrupted basis and to identify criminal suspects, businesses and assets of targets of investigations for potential arrest, seizure and forfeiture will require the usage of a robust investigative database subscription service.

The scope of this requirement is to subscribe to and use the contractor's proprietary data, content and analytical data to optimize ICE operational support functions to enable mission success. This includes supporting all aspects of ICE screening and vetting, lead development, and criminal analysis activities. It also includes, but is not limited to, conducting data extractions to identify unusual trends, data anomalies, and control breakdowns, identifying possible trends, patterns, and links to automate methods for detecting, monitoring, analyzing, summarizing and graphically representing patterns of relationships between entities, identifying potentially criminal and fraudulent behavior before crime and fraud can materialize, and detecting and reporting elements of crimes involving the exploitation or attempts to exploit the immigration and customs laws of the United States.

ICE requires web-based law enforcement investigative databases platform to provide constant (24 hour, seven days per week, 365 days a year) accessibility to a database for ICE law enforcement personnel across the United States in the execution of their official law enforcement duties.

The task areas listed constitute the technical scope of this PWS:

- Task Area 1: Database Functionality Requirements (CLIN 0001)
- Task Area 1A: Training and User Management Support (CLIN 0002)
- Task Area 2: License Plate Reader (LPR) (CLIN 0003)
- Task Area 2A: License Plate Reader Training and User Management Support (CLIN 0004)

Contractor shall provide database access to 11,000 users.

3.0 TASK REQUIREMENTS

The ICE law enforcement investigative database platform shall contain a web-based, centralized database for client management and reporting. Generally, all users shall provide direct input into the database and output requests (reports) shall be generated directly from the database system.

The ICE participating programs shall provide input (i.e., client level data) and the contractor shall provide the database systems administrative and support for report generation. The investigative platform requires the best-supported investigative data and data-analytic

management available in the marketplace; to allow readily available access to billions of public records and additional investigative content in an intuitive working environment.

The tasks required under this Performance Work Statement (PWS) require a community-wide data-analytic collection and management system that includes the following:

3.1 TASK AREA 1: DATABASE FUNCTIONAL REQUIREMENTS

- The government's requirement is that the database uses a matching algorithm to return search records that can identify and eliminate duplicated results. The database shall use Entity Resolution applied across results from all sources as they are returned. This maximizes the value of searching multiple sources and saves time by automating the process of record comparison.
- The government's requirement is that the database must be able to interface with Palantir FALCON and RAVEn core systems as well as other external data collection systems such as PenLink. The database program shall offer a system-to-system (S2S) connection that merges the database program public's and proprietary data with the agency investigative platforms or external data systems to narrow in and locate persons and assets of interest. (S2S application-programming interface (API) will replace Palantir connection).
- The government's requirement is that the database must compare the input search criteria and score them against all records in their data sources. The database must use a Relevant Scoring application that allows them to return the most relevant and most current records at the top of the results list.
- The government's requirement is that the database program must have the ability to construct link charts. The database shall use Link-Chart Visualization and Mapping, which allows investigators to save selected results and report data indefinitely and provides the capability to generate link charts and map views of the data.
- The government's requirement is that the database program must allow for multiple searches using unique criteria. Investigators must be allowed to enter specific search criteria once, the system then returns all relevant data, regardless of the source. The program must support search federation against both open-source and internal data repositories and include features like entity resolution, search filtering and charting and mapping across all supported sources.
- The government's requirement is that the database program must allow for Batch Requests where multiple social security numbers (SSN) and or phone numbers may be queried at one time. This capability is both time- and cost-saving for Worksite and Identity Benefit Fraud investigations where multiple SSN's are queried at one time vs. one at a time.
- The government's requirement is that the database must allow for mobile "on the go" access. The law enforcement investigative research tool shall provide full access to core search and report capability from mobile, wireless devices, including HTML5-supported smartphones.
- Available functionality includes person, vehicle, watercraft and phone searches and the National Comprehensive Report. Reports shall be saved automatically in a

results tab for future viewing.

- The government's requirement is that the database shall have the ability to conform to the investigator's needs, so reports generated can be customized to an investigator or analyst case load. Users shall create report templates by setting report preferences, identifying which sections to include, and setting the sequence in which sections are displayed. For example, customers wanting to see only the asset-related information for an individual could create an "Asset Profile" report with the sections they want included, in the order that they want. The law enforcement online research tool shall also offer a workspace feature which allows users to save selected results and report data indefinitely and provides the ability to generate link-chart and map views of the data. Visualizing information on multiple subjects in a link-chart view makes it easier for investigators to discern possible connections or associations between subjects/entities.
- The government's requirement is that the information provided by the law enforcement online research tool should enable ICE to effectively and quickly identify assets currently owned or previously owned/operated by suspect individuals and/or organizations under investigation. The research tool should allow for the flexibility of locating suspects' assets through a multitude of search options. It should also offer the ability to create custom searches so investigators can retrieve information more specific to the time of criminal activity and/or by target name.
- The government's requirement is that the information provided by the law enforcement online research tool should enable ICE OPR to effectively identify searching of a record/document and generate a corresponding audit record. The system shall allow OPR to search sign-on data for the user profile based on a beginning and ending date and time.

- The government's requirement is the system will have the capacity to:
    - Generate program, agency, community, and, if applicable, collaborative level reports.
    - Produce standard, built-in reports and forms to be queried by Area of Responsibility (AOR), to include user reports, agency reports, component, location and sublocation reports and other reports as required.
    - Perform integrated ad hoc reporting that maintains user level security restrictions while allowing for user flexibility in choosing tables and fields as well as filtering and conditional report aspects.
    - Import and export data through XML and CSV formats, imports and exports and ability to securely strip data of identifiers and manage data transmission.
- The government's requirement is that System Security will include Integrated technical safeguards to ensure a high level of privacy and security, including:
    - Back end server(s), including data encryption and transmission
    - Administrator controlled username and password access
    - Automatic timeout/log-off
    - Administrator controlled user level read, write, edit and delete capabilities

- Administrator controlled user level module and sub-module access
- Automated audit trail
- Information Security Industry Standard encryption and SSL certifications (256-Bit AES encryption)

All technical safeguards required to protect Personally Identifiable Information (PII) All security safeguards required for compliance.

3.2 TASK AREA 2: LICENSE PLATE READER (LPR) REQUIREMENTS

- The LPR data service shall contain LPR records from a variety of sources across the United States, such as publicly accessible toll roads or parking lot cameras, vehicles repossession companies and law enforcement agencies.
- The LPR data service shall include substantial unique LPR detection records.
- The LPR data service shall compile LPR from at least 25 states and 24 of the top 30 most populous metropolitan statistical areas to the extend authorized by law in those locations.
    - A metropolitan statistical area is defined as: a geographical region with a relatively high population density at its core and close economic ties throughout the area as defined by the Office of Management and Budget (OMB) and used by the Census Bureau and other federal government agencies for statistical purposes.
- The LPR data service provider shall demonstrate the number of new unique records that were added to the commercially available LPR database each month for the last consecutive twelve (12) months.
- The LPR data service shall make available at least 30 million new unique LPR data records each month.

3.2.1 QUERY CAPABILITIES

- The contract shall ensure that before a user is able to perform a query from the database or mobile application; the tool must display upon logon a splash screen that describes the agency's permissible uses of the database application, the data and all user's affirmative consent to the rules of behavior prior to initial entry of the investigative tool.
- The contractor shall ensure the splash screen shall appear at each logon event.
- The contractor shall ensure the text on the splash screen shall also be available to the users via a hyperlink within the main system interface (to include mobile app interface)
- The contractor shall provide the language for the splash screen content.
- The contractor shall ensure that queries of the LPR data service can be based on a complete or partial license plate number queried by the user only and the data returned in response must be limited to matches of that license plate number only within the specified period of time.
- The contractor shall create separate log-on environments for ICE personnel authorized to perform advanced queries. One environment will appear for users who must enter a license plate number (full or partial) or other non-geographical

coordinate based restrictions to query the database, and the other environment will appear for users authorized to search by geographic area.

- The query interface shall include a drop-down field for users to select a reason code for the query from a pre-populated list. The specific reason codes shall be provided by ICE. This field is mandatory for conducting a query.
- The contractor shall ensure geographic queries also include a common plate search feature. A common plate search allows investigators to analyze multiple locations to see if any license plate(s) appeared in the selected locations.
- The query interface will require the user to identify whether the user is entering data for either him or herself or for another individual. If the user is entering data for another individual, the query interface will require the user to enter the name of the other individual.
- The query interface must include a free-text field of at least 255 alphanumeric characters for user notes. This will allow for additional information that will assist ICE in referencing the specific case for which the query was performed. Completing this field shall be mandatory for conducting a query.
- The system will have the capability to limit the query by time frame to allow users to comply with agency policy. Depending on the type of investigation being conducted, agency policy will allow the user to query the historical LPR detection records for only a certain period of time (e.g., going back 5 years from the date of query for any immigration investigation).
    - The query interface will have a field for the user to select or input the appropriate timeframe for the query.
    - The system will display results only for LPR detection records within that timeframe (e.g., only for the last 5 years).
    - The system shall not run a query that lacks a time frame entered by the user.
        - The contractor shall guarantee the results of queries meet a high degree of accuracy in datasets, with a margin of error not more than 2%.
        - To ensure accuracy of information, the response to a query must include at least two photos on all hits.
        - Photos must be of sufficient quality to allow the user to visually confirm the license plate and vehicle make/model in the photo are the same as what is represented in the contractor system.
        - Query results must seamlessly integrate with web-based interactive maps. The printable report should show two different map views, nearest address, nearest intersection and coordinates.
        - The contractor shall provide a notification mechanism in the event ICE users identify photographs that do not match the data in their system (license plate numbers or make/model mismatches). The contractor shall address all erroneous data. The contractor shall notify ICE and the ICE user of any inputted erroneous data and keep ICE and ICE users informed of corrections to erroneous data.

- The contractor will not use any information provided by the agency (query data) for its own purposes or share the information with other customers, business partners, or any other entity.

- The contractor will not use ICE's queries (the license plate numbers input into the system) for its commercial purposes. The contractor will only use the queries submitted by ICE to maintain an audit log.
- The contractor will ensure ICE user queries are conducted anonymously to ensure other individuals or entities that use the LPR service (whether a law enforcement agency, commercial entity, or otherwise) are not able to identify that ICE is investigating a license plate.

3.2.2 ALERT LIST CAPABILITIES

- The LPR data service shall provide an "Alert List" feature that will save license plate numbers to query them against new records loaded into the contractor's LPR database on an on-going basis. Any matches will result in a near real-time notification to the user who queried the license plate number.
- The LPR data service Alert List will provide capabilities to share Alert List notifications between ICE users involved in the investigation.
- The Alert List feature will: 1) Automatically match new incoming detection records to user-uploaded or -entered Alert Lists containing the license plate numbers of interest in the investigation; 2) Send an email notification to the user originating such Alert List records and to any ICE user that has been shared the Alert List indicating there is a license plate match to new records in the system; and 3) Provide within the LPR system for download a PDF case file report for the match (with maps, vehicle images, and all pertinent detection & Alert List record information) for each email alert notification. The notification must be able to be limited to the user or a user group of ICE law enforcement officers involved in the specific investigation. The notification will comply with all applicable laws, including the Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725.
- The LPR data service will allow specifically designated users to batch upload a maximum of 2,500 license plate records into the "Alert List". The batch upload will be in the form of a single comma separated variable (CSV) file with data fields to include, but not limited to the following: Plate number; State of Registration; Vehicle Year, Make, Model & Color; reason code and an open text field, of at least 255 alphanumeric characters for a user note to assist in referencing the specific purpose / investigation / operation for which the query was performed.
- The contractor will provide the ability to establish Alert List submissions, flag license plates for deconfliction, and perform searches, all conducted anonymously, to ensure other individuals or entities that use the LPR service (whether a law enforcement agency, commercial entity, or otherwise) are not able to identify that ICE is investigating a license plate.
- License plate pictures taken with the automated Optical Character Recognition (OCR) plate number translation shall be submitted to the LPR data service system for matching with license plates on any current ICE Alert List. Any positive matches shall return to the iOS application (identified below) alerting authorized users of a positive match. These pictures will be uploaded into the data service query by an authorized ICE user along with any mandatory information needed for a normal query.

- Each license plate number on an Alert List will be valid for one year unless the user removes it before expiration. The system will prompt users prior to expiration and allow the user to keep the particular Alert List or license plate number active or be given the option to delete the license plate from the Alert List. If the user does not renew, the system shall remove the license plate number from the Alert List.
- All Alert List activity shall be audited to capture username, date and time, reason code, and user note associated with the query, as well as license plate number entry, deletion, renewal, and expiration from the alert list.
- Have quick access and recall of any queries and Alert Lists associated with the user or designated user group. The contractor application will delete any saved data on the mobile device after 60 days, if not already deleted manually by the user.
- The contractor shall not retain any data entered onto an Alert List except as part of the audit trail once the entry has expired per the process described above, or once the user has deleted the entry from the Alert List.

3.2.3 MOBILE DEVICE CAPABILITIES

- The LPR data service shall feature an iOS-compatible mobile application that allows authorized ICE users to:
- Query the LPR data service by entering the license plate number (complete/partial), state of registration, reason code, and the ability to add returned positive matches into the Alert List.
- The contractor shall ensure the mobile application allows the user to scan vehicle plates (full and/or partial), using their mobile device camera, which are automatically uploaded into the contractor's database and queried against various hotlists in the existing IOS/Android compatible applications.
- The contractor shall ensure the mobile application has a mobile alert feature. Scanned plates are sent as detections to the contractor's law enforcement archival and reporting network which could trigger alert notifications. The mobile alert shall enable an alert banner display in near real time if a scanned plate is a shared hot list match.
- Queries can be performed by inputting geographic area (for authorized users).
- The mobile application will conform all other performance, privacy, and functional requirements identified in the PWS. The contractor shall coordinate with ICE to make sure that the mobile application undergoes the required privacy assessment prior to use.

3.2.4 AUDIT AND REPORTING CAPABILITIES

- The contractor shall generate an immutable audit log in electronic form that chronicles the following data:
    - Identity of the user initiating the query or the person on whose behalf the query is initiated, if different;
    - Exact query entered, to include license plate number, date limitations, geographic limitations (if applicable), reason code, and any other data selected or input by the user;

- Date and time of query; and
- Results of the query.

- All Alert List activity shall be audited to capture username, date and time, reason code, and user note associated with the query, as well as license plate number entry, deletion, renewal, and expiration from the alert list.

- The contractor shall provide to ICE user audit reports upon request. Audit reports shall contain the audit log information of a given user(s) for the specified period of time. The contractor shall provide the audit log in electronic form via secure transmission to ICE promptly upon request. The format of the audit log shall allow for ICE to retrieve user activity by username (or ID), query entered (e.g., particular license plate) and date/time. The exact technical requirements and format for the audit log will be negotiated after contract award.

- The contractor shall promptly cooperate with an ICE request to retrieve and provide a copy of the actual records retrieved from the LPR data service in response to a particular query, or any other data relevant to user activity on the contractor system, for purposes of the agency's internal investigations and oversight.

- The contractor shall not use audit trail data for any purpose other than those specified and authorized in this contract.

- The contractor is to provide monthly and upon request, statistics based on positive hits against the number of requested searches and hit list.

- The audit logs specified in this statement of work are records under the Federal Records Act. The contractor shall maintain these records on behalf of ICE throughout the life of the contract, but for no more than seven (7) years. The contractor is not authorized to share these records, or the Alert List data, with any outside entities including other law enforcement agencies. At the end of the contract, the contractor shall extract, transfer, and load these records (including any still-active Alert List data, if requested by ICE) to another storage medium or location specified by ICE. This transfer of records shall occur no later than thirty (30) days after the contract ends. After successful transfer of these records, the contractor shall ensure all copies of the records (including any still-active Alert List data) are securely deleted from all networks and storage media under its control or under the control of any of its agents or subcontractors.

- The contractor shall meet the following Key Performance Parameters (KPPs):

Metric	Unit of Measure	Minimum
LPR Data Service	Uptime – Unit of measure 100%	>99.0
	Operating Schedule	24/7/365
	Scheduled downtime	</= 4 hours per month
	Meantime between failure (MTBF)	4,000 operating hours

Overall Support Service	Support availability	24/7/365
Results of LPR Query	Results of a single LPR query	</= 5 seconds after submission

3.3 TASK AREAS 1A and 2A: TRAINING AND USER MANAGEMENT SUPPORT.

The object of this task is to provide training to ICE personnel through on-site, remote, and/or on-demand training on the Law Enforcement Investigative database tool. Training and user management support is implemented to ensure proper guidance and navigation of the database tool is accessible to all assigned users.

- The contract shall provide written instruction manuals and guidance to facilitate use of the database investigative tool and the LPR system.

- The contract shall ensure the user has the ability to compare new user requests with lists of personnel authorized by ICE to utilize the database and LPR tool.

- The contractor shall ensure that all users has automatic verification of accounts with the ability to audit by using the user's Originating Agency Identifier (ORI) to be matched against a current real-time list of active ORI numbers provided directly or indirectly by the National Law Enforcement Telecommunications System (NLETS).

- The contractor shall have the ability to add new users or delete existing users within 24 business hours of ICEs request.

- The contract shall provide initial training or subsequent training to orient persons to the use of the database investigative and LPR tool; to include the "Help Desk" support related to the use, access and maintenance of the tool.

- The contractor shall provide customized training on-site, telephone and web-based training to include webinars and "on demand" classes and electronic quick reference guides for users. On-site training shall be limited to the Washington, DC location with a maximum of 2 training visits per year.

- The contract shall provide system training and escalation procedures as it pertains to agency administrators and shall include procedures for password resets to the database tool.

- The contractor shall provide unlimited technical support for all users.

- The contractor shall perform periodic or as needed updates (maintenance, refresh, etc.) to the overall database tool, web-based interface and mobile application. The contractor shall also ensure to employ appropriate technical, administrative and physical security controls are in place to protect the integrity, availability and confidentiality of the data that resides on all of its systems.

4.0 OTHER APPLICABLE REQUIREMENTS

4.1 PERIOD OF PERFORMANCE

The Period of Performance will consist of a base year with four (4) one-year options.

4.2 PLACE OF PERFORMANCE

The primary place of performance will be the Contractor's facilities with frequent visits to the, Immigration and Customs Enforcement (ICE) headquarters facilities in the Washington Metro Area.

4.3 TRAVEL

Contractor travel is not required for this requirement. Local meetings or activities planned outside of the defined place of performance are permitted, but all expenses incurred are the responsibility of the contractor.

4.4 POST AWARD CONFERENCE

The Contractor shall attend Post Award Conference with the Contracting Officer and the COR no later than 5 business days after the date of award. The purpose of the Post Award Conference, which will be chaired by the Contracting Officer, is to discuss technical and contracting objectives of this contract. The Post Award Conference will be held either virtually (e.g., MS Teams, Zoom, Adobe Connect, etc.) and/or at the Government's facility, location to be determined via teleconference.

4.5 INVOICES

A standard invoice template shall be provided by the contractor and confirmed by the COR for use on this contract. Invoices shall be verified by the Government COR and submitted on a monthly basis.

4.6 CONTRACTOR QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

The Contractor shall establish and maintain a Quality Assurance Surveillance Plan (QASP) to ensure the requirements of this contract are provided as specified. The Contractor shall provide a QASP describing the inspection system that they intend to use for the requested services listed. The contractor shall implement procedures to identify, prevent and ensure non-recurrence of defective services. The Contractor's draft QASP shall be required as part of their quote submittal. The CO will notify the Contractor of acceptance or the necessity for QASP modification of the plan no later than 10 business days after award. The Contractor shall provide a final QASP to the COR no later than 20 business days after award. The QASP shall be updated as changes occur and shall be submitted to the COR for review and subsequent CO acceptance by the government. The Performance Requirements Summary (PRS) and Performance Standards Matrix (PSM) is outlined in the Quality Assurance Surveillance Plan (QASP) Appendix A.

5.0 DELIVERABLES

The contractor shall provide the following deliverables in the format and frequency listed.

Deliverables Name	PWS Paragraph	Frequency
Kick-off Meeting/Post Award Conference	4.4	A kick-off meeting with the government will be conducted within 5 days of award. Meeting minutes due from Contractor to COR & CO within 2 business days of the meeting.
Audit report, ad hoc reports, user manuals, etc.	3.2.4 3.3	Reports are due upon request of the COR and/or as required. To include any subsequent updates.
Audit Logs, transfer of records	3.2.4	Provide email confirmation 30 days after contract ends.
Data Rights any work first produced such as user administrative and operations manuals and anything else first produced under this PWS if applicable.		One month prior to the end of the period of performance (POP).
QASP/Progress Reports	4.7	Draft due to the government proposal. Final QASP due to the COR and CO 20 days after award. Subsequent reports due quarterly and/or as requested.
Invoices	4.5	Invoice should be submitted on a monthly basis to the COR and designated Finance Center for all services performed and no more than 30 days in the arrears of the last day of the POP.

5.1 GENERAL REPORT REQUIREMENTS

The Contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with ICE workstations (Windows XP and Microsoft Office Applications).

5.2 ACCEPTANCE CRITERIA

ICE will accept or reject deliverables within fifteen (15) business days after delivery. If rejected, the Contractor shall make corrections as specified and resubmit the deliverable for review and approval within five (5) business days provided however that contractor is not dependent upon a third party for performance. If the government does not reply within the specific timeframe than the deliverable shall be determined acceptable.

6.0 SECTION 508 COMPLIANCE

Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) as amended by P.L. 105-220 under Title IV (Rehabilitation Act Amendments of 1998) all Electronic and Information Technology (EIT) developed, procured, maintained and/or used under this contract shall be in compliance with the "Electronic and Information Technology Accessibility Standards" set forth by the Architectural and Transportation Barriers Compliance Board (also referred to as the "Access Board") in 36 CFR Part 1194. The complete text of Section 508 Standards can be accessed at http://www.access-board.gov/ or at http://www.section508.gov.

7.0 PRIVACY REQUIREMENTS

Limiting Access to Privacy Act and Other Sensitive Information
In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984), and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires contractor personnel to have access to information protected by the Privacy Act of 1974, the contractor is advised that the relevant DHS system of records notices (SORNs) applicable to this Privacy Act information may be found at https://www.dhs.gov/system-records-notices-sorns. Applicable SORNS of other agencies may be accessed through the agencies' websites or by searching GovInfo, available at https://www.govinfo.gov that replaced the FDsys website in December 2018. SORNs may be updated at any time.

Prohibition on Performing Work Outside a Government Facility/Network/Equipment
The Contractor shall perform all tasks on authorized Government networks, using Government-furnished IT and other equipment and/or Workplace as a Service (WaaS) if WaaS is authorized by the statement of work. Government information shall remain within the confines of authorized Government networks at all times. Except where telework is specifically authorized within this contract, the Contractor shall perform all tasks described in this document at authorized Government facilities; the Contractor is prohibited from performing these tasks at or removing Government-furnished information to any other facility; and Government information shall remain within the confines of authorized Government facilities at all times. Contractors may only access classified materials on government furnished equipment in authorized government owned facilities regardless of telework authorizations.

Prior Approval Required to Hire Subcontractors
The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (Subcontractor) in support of this contract requiring the disclosure of

information, documentary material and/or records generated under or relating to this contract. The Contractor (and any Subcontractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

Separation Checklist for Contractor Employees
Contractor shall complete a separation checklist before any employee or Subcontractor employee terminates working on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposal of sensitive personally identifiable information (PII), in paper or electronic form, in the custody of the employee or Subcontractor employee including the sanitization of data on any computer systems or media as appropriate; and (3) termination of any technological access to the Contractor's facilities or systems that would permit the terminated employee's access to sensitive PII.
In the event of adverse job actions resulting in the dismissal of an employee or Subcontractor employee, the Contractor shall notify the Contracting Officer's Representative (COR) within 24 hours. For normal separations, the Contractor shall submit the checklist on the last day of employment or work on the contract.

As requested, contractors shall assist the ICE Point of Contact (ICE/POC), Contracting Officer, or COR with completing ICE Form 50-005/Contractor Employee Separation Clearance Checklist by returning all Government-furnished property including but not limited to computer equipment, media, credentials and passports, smart cards, mobile devices, PIV cards, calling cards, and keys and terminating access to all user accounts and systems.

Contractor's Commercial License Agreement and Government Electronic Information Rights
Except as stated in the Performance Work Statement and, where applicable, the Contractor's Commercial License Agreement, the Government Agency owns the rights to all electronic information (electronic data, electronic information systems or electronic databases) and all supporting documentation and associated metadata created as part of this contract. All deliverables (including all data and records) under the contract are the property of the U.S. Government and are considered federal records, for which the Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

Privacy Lead Requirements
If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy documentation, the Contractor shall assign or procure a Privacy Lead, to be listed under the SOW or PWS's required Contractor Personnel section. The Privacy Lead shall be responsible for providing adequate support to DHS to ensure DHS can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance. The Privacy Lead shall work with personnel from the program office, the ICE Privacy Unit, the Office of the Chief Information Officer, and the Records and Data Management Unit to ensure that the privacy documentation is kept on schedule, that the answers to questions in the PIA are thorough and complete, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.

The Privacy Lead:

- Must have excellent writing skills, the ability to explain technology clearly for a non-technical audience, and the ability to synthesize information from a variety of sources.
- Must have excellent verbal communication and organizational skills.
- Must have experience writing PIAs. Ideally the candidate would have experience writing PIAs for DHS.
- Must be knowledgeable about the Privacy Act of 1974 and the E-Government Act of 2002.
- Must be able to work well with others.

If a Privacy Lead is already in place with the program office and the contract involves IT system builds or substantial changes that may require privacy documentation, the requirement for a separate Private Lead specifically assigned under this contract may be waived provided the Contractor agrees to have the existing Privacy Lead coordinate with and support the ICE Privacy POC to ensure privacy concerns are proactively reviewed and so ICE can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance if required. The Contractor shall work with personnel from the program office, the ICE Office of Information Governance and Privacy, and the Office of the Chief Information Officer to ensure that the privacy documentation is kept on schedule, that the answers to questions in any privacy documents are thorough and complete, that all records management requirements are met, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.

Performance Work Statement (PWS)
Department of Homeland Security (DHS),
Immigration and Customs Enforcement (ICE)
Law Enforcement Investigative Database Subscription
December 10, 2020

1. BACKGROUND

The intent of this Performance Work Statement (PWS) is to procure a web-based law enforcement investigative database subscription service to assist Immigration, Customs and Enforcement (ICE) mission of conducting criminal investigations that protect the United States against terrorists and criminal organizations that threaten our safety and national security; to combat transnational criminal enterprises that see to exploit America's legitimate trade, travel and financial systems. ICE investigative agents require a robust analytical research tool for its in-depth exploration of persons of interest and vehicles.

The purpose of this contract is to provide ICE agents an investigative database system to further strategize arrests to minimize and, in some cases, avoid impact of potential injury. ICE requirement of a web-based law enforcement investigative database platform is to include, integration access to public records and commercial data with uninterrupted service, integrate investigative capabilities with the license plate recognition capabilities to be utilized by multiple ICE Directorates to include but not limited to Homeland Security Investigative (HSI), Enforcement and Removal Operations (ERO) and Office of Professional Responsibility (OPR). Use of this database subscription services furthers the criminal law enforcement mission.

1.1 **DHS/ICE**

ICE is the largest investigative agency in the Department of Homeland Security (DHS) and was formally established on March 1, 2003. ICE's primary mission is to protect national security, public safety, and the integrity of the US borders through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration.

ICE investigates a range of domestic and international activities including:

- Human smuggling and trafficking;
- Narcotics, cultural property, weapons and other contraband smuggling;
- Export enforcement, e.g., illegal arms and dual-use equipment;
- Financial crimes;
- Commercial fraud;
- Intellectual property rights violations;
- Cyber-crimes;
- Immigration fraud; and,
- Human rights violations.

The law enforcement investigative database system currently supports over 11,000 users across multiple program areas with analytical data and concrete information to search high risk and

politically exposed criminal activity worldwide. The database subscription service plays a crucial role in ICEs overall investigative mission success. Moreover, the agency can achieve cost savings to the government when reducing the work hours required for physical surveillance.

2.0 SCOPE/OBJECTIVES

The Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement (ICE) houses a large dataset of detailed data that is available to an assortment of approved law enforcement users. ICE criminal law enforcement mission; to enhance investigations to support all mission activities mentioned above in over 50 countries and 67 locations globally; to provide a platform where the continuity of public records and commercial data is available on an uninterrupted basis and to identify criminal suspects, businesses and assets of targets of investigations for potential arrest, seizure and forfeiture will require the usage of a robust investigative database subscription service.

The scope of this requirement is to subscribe to and use the contractor's proprietary data, content and analytical data to optimize ICE operational support functions to enable mission success. This includes supporting all aspects of ICE screening and vetting, lead development, and criminal analysis activities. It also includes, but is not limited to, conducting data extractions to identify unusual trends, data anomalies, and control breakdowns, identifying possible trends, patterns, and links to automate methods for detecting, monitoring, analyzing, summarizing and graphically representing patterns of relationships between entities, identifying potentially criminal and fraudulent behavior before crime and fraud can materialize, and detecting and reporting elements of crimes involving the exploitation or attempts to exploit the immigration and customs laws of the United States.

ICE requires web-based law enforcement investigative databases platform to provide constant (24 hour, seven days per week, 365 days a year) accessibility to a database for ICE law enforcement personnel across the United States in the execution of their official law enforcement duties.

The task areas listed constitute the technical scope of this PWS:

- Task Area 1: Database Functionality Requirements (CLIN 0001)
- Task Area 1A: Training and User Management Support (CLIN 0002)
- Task Area 2: License Plate Reader (LPR) (CLIN 0003)
- Task Area 2A: License Plate Reader Training and User Management Support (CLIN 0004)

Contractor shall provide database access to 11,000 users.

3.0 TASK REQUIREMENTS

The ICE law enforcement investigative database platform shall contain a web-based, centralized database for client management and reporting. Generally, all users shall provide direct input into the database and output requests (reports) shall be generated directly from the database system.

The ICE participating programs shall provide input (i.e., client level data) and the contractor shall provide the database systems administrative and support for report generation. The

investigative platform requires the best-supported investigative data and data-analytic management available in the marketplace; to allow readily available access to billions of public records and additional investigative content in an intuitive working environment.

The tasks required under this Performance Work Statement (PWS) require a community-wide data-analytic collection and management system that includes the following:

3.1 TASK AREA 1: DATABASE FUNCTIONAL REQUIREMENTS

- The government's requirement is that the database uses a matching algorithm to return search records that can identify and eliminate duplicated results. The database shall use Entity Resolution applied across results from all sources as they are returned. This maximizes the value of searching multiple sources and saves time by automating the process of record comparison.
- The government's requirement is that the database must be able to interface with Palantir FALCON and RAVEn core systems. The database program shall offer a system-to-system (S2S) connection that merges the database program public's and proprietary data with the agency investigative platforms to narrow in and locate persons and assets of interest. (S2S application-programming interface (API) will replace Palantir connection).
- The government's requirement is that the database must compare the input search criteria and score them against all records in their data sources. The database must use a Relevant Scoring application that allows them to return the most relevant and most current records at the top of the results list.
- The government's requirement is that the database program must have the ability to construct link charts. The database shall use Link-Chart Visualization and Mapping, which allows investigators to save selected results and report data indefinitely and provides the capability to generate link charts and map views of the data.
- The government's requirement is that the database program must allow for multiple searches using unique criteria. Investigators must be allowed to enter specific search criteria once, the system then returns all relevant data, regardless of the source. The program must support search federation against both open-source and internal data repositories and include features like entity resolution, search filtering and charting and mapping across all supported sources.
- The government's requirement is that the database program must allow for Batch Requests where multiple social security numbers (SSN) and or phone numbers may be queried at one time. This capability is both time- and cost-saving for Worksite and Identity Benefit Fraud investigations where multiple SSN's are queried at one time vs. one at a time.
- The government's requirement is that the database must allow for mobile "on the go" access. The law enforcement investigative research tool shall provide full access to core search and report capability from mobile, wireless devices, including HTML5-supported smartphones.
- Available functionality includes person, vehicle, watercraft and phone searches and the National Comprehensive Report. Reports shall be saved automatically in a

results tab for future viewing.

- The government's requirement is that the database shall have the ability to conform to the investigator's needs, so reports generated can be customized to an investigator or analyst case load. Users shall create report templates by setting report preferences, identifying which sections to include, and setting the sequence in which sections are displayed. For example, customers wanting to see only the asset-related information for an individual could create an "Asset Profile" report with the sections they want included, in the order that they want. The law enforcement online research tool shall also offer a workspace feature which allows users to save selected results and report data indefinitely and provides the ability to generate link-chart and map views of the data. Visualizing information on multiple subjects in a link-chart view makes it easier for investigators to discern possible connections or associations between subjects/entities.
- The government's requirement is that the information provided by the law enforcement online research tool should enable ICE to effectively and quickly identify assets currently owned or previously owned/operated by suspect individuals and/or organizations under investigation. The research tool should allow for the flexibility of locating suspects' assets through a multitude of search options. It should also offer the ability to create custom searches so investigators can retrieve information more specific to the time of criminal activity and/or by target name.
- The government's requirement is that the information provided by the law enforcement online research tool should enable ICE OPR to effectively identify searching of a record/document and generate a corresponding audit record. The system shall allow OPR to search sign-on data for the user profile based on a beginning and ending date and time.

- The government's requirement is the system will have the capacity to:
    - Generate program, agency, community, and, if applicable, collaborative level reports.
    - Produce standard, built-in reports and forms to be queried by Area of Responsibility (AOR), to include user reports, agency reports, component, location and sublocation reports and other reports as required.
    - Perform integrated ad hoc reporting that maintains user level security restrictions while allowing for user flexibility in choosing tables and fields as well as filtering and conditional report aspects.
    - Import and export data through XML and CSV formats, imports and exports and ability to securely strip data of identifiers and manage data transmission.
- The government's requirement is that System Security will include Integrated technical safeguards to ensure a high level of privacy and security, including:
    - Back end server(s), including data encryption and transmission
    - Administrator controlled username and password access
    - Automatic timeout/log-off
    - Administrator controlled user level read, write, edit and delete capabilities

- Administrator controlled user level module and sub-module access
- Automated audit trail
- Information Security Industry Standard encryption and SSL certifications (256-Bit AES encryption)

All technical safeguards required to protect Personally Identifiable Information (PII) All security safeguards required for compliance.

3.2 TASK AREA 2: LICENSE PLATE READER (LPR) REQUIREMENTS

- The LPR data service shall contain LPR records from a variety of sources across the United States, such as publicly accessible toll roads or parking lot cameras, vehicles repossession companies and law enforcement agencies.
- The LPR data service shall include substantial unique LPR detection records.
- The LPR data service shall compile LPR from at least 25 states and 24 of the top 30 most populous metropolitan statistical areas to the extend authorized by law in those locations.
    - A metropolitan statistical area is defined as: a geographical region with a relatively high population density at its core and close economic ties throughout the area as defined by the Office of Management and Budget (OMB) and used by the Census Bureau and other federal government agencies for statistical purposes.
- The LPR data service provider shall demonstrate the number of new unique records that were added to the commercially available LPR database each month for the last consecutive twelve (12) months.
- The LPR data service shall make available at least 30 million new unique LPR data records each month.

3.2.1 QUERY CAPABILITIES

- The contract shall ensure that before a user is able to perform a query from the database or mobile application; the tool must display upon logon a splash screen that describes the agency's permissible uses of the database application, the data and all user's affirmative consent to the rules of behavior prior to initial entry of the investigative tool.
- The contractor shall ensure the splash screen shall appear at each logon event.
- The contractor shall ensure the text on the splash screen shall also be available to the users via a hyperlink within the main system interface (to include mobile app interface)
- The contractor shall provide the language for the splash screen content.
- The contractor shall ensure that queries of the LPR data service can be based on a complete or partial license plate number queried by the user only and the data returned in response must be limited to matches of that license plate number only within the specified period of time.
- The contractor shall create separate log-on environments for ICE personnel authorized to perform advanced queries. One environment will appear for users who must enter a license plate number (full or partial) or other non-geographical

coordinate based restrictions to query the database, and the other environment will appear for users authorized to search by geographic area.

- The query interface shall include a drop-down field for users to select a reason code for the query from a pre-populated list. The specific reason codes shall be provided by ICE. This field is mandatory for conducting a query.
- The contractor shall ensure geographic queries also include a common plate search feature. A common plate search allows investigators to analyze multiple locations to see if any license plate(s) appeared in the selected locations.
- The query interface will require the user to identify whether the user is entering data for either him or herself or for another individual. If the user is entering data for another individual, the query interface will require the user to enter the name of the other individual.
- The query interface must include a free-text field of at least 255 alphanumeric characters for user notes. This will allow for additional information that will assist ICE in referencing the specific case for which the query was performed. Completing this field shall be mandatory for conducting a query.
- The system will have the capability to limit the query by time frame to allow users to comply with agency policy. Depending on the type of investigation being conducted, agency policy will allow the user to query the historical LPR detection records for only a certain period of time (e.g., going back 5 years from the date of query for any immigration investigation).
    - The query interface will have a field for the user to select or input the appropriate timeframe for the query.
    - The system will display results only for LPR detection records within that timeframe (e.g., only for the last 5 years).
    - The system shall not run a query that lacks a time frame entered by the user.
        - The contractor shall guarantee the results of queries meet a high degree of accuracy in datasets, with a margin of error not more than 2%.
        - To ensure accuracy of information, the response to a query must include at least two photos on all hits.
        - Photos must be of sufficient quality to allow the user to visually confirm the license plate and vehicle make/model in the photo are the same as what is represented in the contractor system.
        - Query results must seamlessly integrate with web-based interactive maps. The printable report should show two different map views, nearest address, nearest intersection and coordinates.
        - The contractor shall provide a notification mechanism in the event ICE users identify photographs that do not match the data in their system (license plate numbers or make/model mismatches). The contractor shall address all erroneous data. The contractor shall notify ICE and the ICE user of any inputted erroneous data and keep ICE and ICE users informed of corrections to erroneous data.

- The contractor will not use any information provided by the agency (query data) for its own purposes or share the information with other customers, business partners, or any other entity.

- The contractor will not use ICE's queries (the license plate numbers input into the system) for its commercial purposes. The contractor will only use the queries submitted by ICE to maintain an audit log.
- The contractor will ensure ICE user queries are conducted anonymously to ensure other individuals or entities that use the LPR service (whether a law enforcement agency, commercial entity, or otherwise) are not able to identify that ICE is investigating a license plate.

3.2.2 ALERT LIST CAPABILITIES

- The LPR data service shall provide an "Alert List" feature that will save license plate numbers to query them against new records loaded into the contractor's LPR database on an on-going basis. Any matches will result in a near real-time notification to the user who queried the license plate number.
- The LPR data service Alert List will provide capabilities to share Alert List notifications between ICE users involved in the investigation.
- The Alert List feature will: 1) Automatically match new incoming detection records to user-uploaded or -entered Alert Lists containing the license plate numbers of interest in the investigation; 2) Send an email notification to the user originating such Alert List records and to any ICE user that has been shared the Alert List indicating there is a license plate match to new records in the system; and 3) Provide within the LPR system for download a PDF case file report for the match (with maps, vehicle images, and all pertinent detection & Alert List record information) for each email alert notification. The notification must be able to be limited to the user or a user group of ICE law enforcement officers involved in the specific investigation. The notification will comply with all applicable laws, including the Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725.
- The LPR data service will allow specifically designated users to batch upload a maximum of 2,500 license plate records into the "Alert List". The batch upload will be in the form of a single comma separated variable (CSV) file with data fields to include, but not limited to the following: Plate number; State of Registration; Vehicle Year, Make, Model & Color; reason code and an open text field, of at least 255 alphanumeric characters for a user note to assist in referencing the specific purpose / investigation / operation for which the query was performed.
- The contractor will provide the ability to establish Alert List submissions, flag license plates for deconfliction, and perform searches, all conducted anonymously, to ensure other individuals or entities that use the LPR service (whether a law enforcement agency, commercial entity, or otherwise) are not able to identify that ICE is investigating a license plate.
- License plate pictures taken with the automated Optical Character Recognition (OCR) plate number translation shall be submitted to the LPR data service system for matching with license plates on any current ICE Alert List. Any positive matches shall return to the iOS application (identified below) alerting authorized users of a positive match. These pictures will be uploaded into the data service query by an authorized ICE user along with any mandatory information needed for a normal query.

- Each license plate number on an Alert List will be valid for one year unless the user removes it before expiration. The system will prompt users prior to expiration and allow the user to keep the particular Alert List or license plate number active or be given the option to delete the license plate from the Alert List. If the user does not renew, the system shall remove the license plate number from the Alert List.
- All Alert List activity shall be audited to capture username, date and time, reason code, and user note associated with the query, as well as license plate number entry, deletion, renewal, and expiration from the alert list.
- Have quick access and recall of any queries and Alert Lists associated with the user or designated user group. The contractor application will delete any saved data on the mobile device after 60 days, if not already deleted manually by the user.
- The contractor shall not retain any data entered onto an Alert List except as part of the audit trail once the entry has expired per the process described above, or once the user has deleted the entry from the Alert List.

3.2.3 MOBILE DEVICE CAPABILITIES

- The LPR data service shall feature an iOS-compatible mobile application that allows authorized ICE users to:
- Query the LPR data service by entering the license plate number (complete/partial), state of registration, reason code, and the ability to add returned positive matches into the Alert List.
- The contractor shall ensure the mobile application allows the user to scan vehicle plates (full and/or partial), using their mobile device camera, which are automatically uploaded into the contractor's database and queried against various hotlists in the existing IOS/Android compatible applications.
- The contractor shall ensure the mobile application has a mobile alert feature. Scanned plates are sent as detections to the contractor's law enforcement archival and reporting network which could trigger alert notifications. The mobile alert shall enable an alert banner display in near real time if a scanned plate is a shared hot list match.
- Queries can be performed by inputting geographic area (for authorized users).
- The mobile application will conform all other performance, privacy, and functional requirements identified in the PWS. The contractor shall coordinate with ICE to make sure that the mobile application undergoes the required privacy assessment prior to use.

3.2.4 AUDIT AND REPORTING CAPABILITIES

- The contractor shall generate an immutable audit log in electronic form that chronicles the following data:
    - Identity of the user initiating the query or the person on whose behalf the query is initiated, if different;
    - Exact query entered, to include license plate number, date limitations, geographic limitations (if applicable), reason code, and any other data selected or input by the user;

- Date and time of query; and
- Results of the query.

- All Alert List activity shall be audited to capture username, date and time, reason code, and user note associated with the query, as well as license plate number entry, deletion, renewal, and expiration from the alert list.

- The contractor shall provide to ICE user audit reports upon request. Audit reports shall contain the audit log information of a given user(s) for the specified period of time. The contractor shall provide the audit log in electronic form via secure transmission to ICE promptly upon request. The format of the audit log shall allow for ICE to retrieve user activity by username (or ID), query entered (e.g., particular license plate) and date/time. The exact technical requirements and format for the audit log will be negotiated after contract award.

- The contractor shall promptly cooperate with an ICE request to retrieve and provide a copy of the actual records retrieved from the LPR data service in response to a particular query, or any other data relevant to user activity on the contractor system, for purposes of the agency's internal investigations and oversight.

- The contractor shall not use audit trail data for any purpose other than those specified and authorized in this contract.

- The contractor is to provide monthly and upon request, statistics based on positive hits against the number of requested searches and hit list.

- The audit logs specified in this statement of work are records under the Federal Records Act. The contractor shall maintain these records on behalf of ICE throughout the life of the contract, but for no more than seven (7) years. The contractor is not authorized to share these records, or the Alert List data, with any outside entities including other law enforcement agencies. At the end of the contract, the contractor shall extract, transfer, and load these records (including any still-active Alert List data, if requested by ICE) to another storage medium or location specified by ICE. This transfer of records shall occur no later than thirty (30) days after the contract ends. After successful transfer of these records, the contractor shall ensure all copies of the records (including any still-active Alert List data) are securely deleted from all networks and storage media under its control or under the control of any of its agents or subcontractors.

- The contractor shall meet the following Key Performance Parameters (KPPs):

Metric	Unit of Measure	Minimum
LPR Data Service	Uptime – Unit of measure 100%	>99.0
	Operating Schedule	24/7/365
	Scheduled downtime	</= 4 hours per month
	Meantime between failure (MTBF)	4,000 operating hours

Overall Support Service	Support availability	24/7/365
Results of LPR Query	Results of a single LPR query	</= 5 seconds after submission

3.3 TASK AREAS 1A and 2A: TRAINING AND USER MANAGEMENT SUPPORT.

The object of this task is to provide training to ICE personnel through on-site, remote, and/or on-demand training on the Law Enforcement Investigative database tool. Training and user management support is implemented to ensure proper guidance and navigation of the database tool is accessible to all assigned users.

- The contract shall provide written instruction manuals and guidance to facilitate use of the database investigative tool and the LPR system.

- The contract shall ensure the user has the ability to compare new user requests with lists of personnel authorized by ICE to utilize the database and LPR tool.

- The contractor shall ensure that all users has automatic verification of accounts with the ability to audit by using the user's Originating Agency Identifier (ORI) to be matched against a current real-time list of active ORI numbers provided directly or indirectly by the National Law Enforcement Telecommunications System (NLETS).

- The contractor shall have the ability to add new users or delete existing users within 24 business hours of ICEs request.

- The contract shall provide initial training or subsequent training to orient persons to the use of the database investigative and LPR tool; to include the "Help Desk" support related to the use, access and maintenance of the tool.

- The contractor shall provide customized training on-site, telephone and web-based training to include webinars and "on demand" classes and electronic quick reference guides for users. On-site training shall be limited to the Washington, DC location with a maximum of 2 training visits per year.

- The contract shall provide system training and escalation procedures as it pertains to agency administrators and shall include procedures for password resets to the database tool.

- The contractor shall provide unlimited technical support for all users.

- The contractor shall perform periodic or as needed updates (maintenance, refresh, etc.) to the overall database tool, web-based interface and mobile application. The contractor shall also ensure to employ appropriate technical, administrative and physical security controls are in place to protect the integrity, availability and confidentiality of the data that resides on all of its systems.

4.0 OTHER APPLICABLE REQUIREMENTS

4.1 PERIOD OF PERFORMANCE

The Period of Performance will consist of a base year with four (4) one-year options.

4.2 PLACE OF PERFORMANCE

The primary place of performance will be the Contractor's facilities with frequent visits to the, Immigration and Customs Enforcement (ICE) headquarters facilities in the Washington Metro Area.

4.3 TRAVEL

Contractor travel is not required for this requirement. Local meetings or activities planned outside of the defined place of performance are permitted, but all expenses incurred are the responsibility of the contractor.

4.4 POST AWARD CONFERENCE

The Contractor shall attend Post Award Conference with the Contracting Officer and the COR no later than 5 business days after the date of award. The purpose of the Post Award Conference, which will be chaired by the Contracting Officer, is to discuss technical and contracting objectives of this contract. The Post Award Conference will be held either virtually (e.g., MS Teams, Zoom, Adobe Connect, etc.) and/or at the Government's facility, location to be determined via teleconference.

4.5 INVOICES

A standard invoice template shall be provided by the contractor and confirmed by the COR for use on this contract. Invoices shall be verified by the Government COR and submitted on a monthly basis.

4.6 CONTRACTOR QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

The Contractor shall establish and maintain a Quality Assurance Surveillance Plan (QASP) to ensure the requirements of this contract are provided as specified. The Contractor shall provide a QASP describing the inspection system that they intend to use for the requested services listed. The contractor shall implement procedures to identify, prevent and ensure non-recurrence of defective services. The Contractor's draft QASP shall be required as part of their quote submittal. The CO will notify the Contractor of acceptance or the necessity for QASP modification of the plan no later than 10 business days after award. The Contractor shall provide a final QASP to the COR no later than 20 business days after award. The QASP shall be updated as changes occur and shall be submitted to the COR for review and subsequent CO acceptance by the government. The Performance Requirements Summary (PRS) and Performance Standards Matrix (PSM) is outlined in the Quality Assurance Surveillance Plan (QASP) Appendix A.

5.0 DELIVERABLES

The contractor shall provide the following deliverables in the format and frequency listed.

Deliverables Name	PWS Paragraph	Frequency
Kick-off Meeting/Post Award Conference	4.4	A kick-off meeting with the government will be conducted within 5 days of award. Meeting minutes due from Contractor to COR & CO within 2 business days of the meeting.
Audit report, ad hoc reports, user manuals, etc.	3.2.4 3.3	Reports are due upon request of the COR and/or as required. To include any subsequent updates.
Audit Logs, transfer of records	3.2.4	Provide email confirmation 30 days after contract ends.
Data Rights any work first produced such as user administrative and operations manuals and anything else first produced under this PWS if applicable.		One month prior to the end of the period of performance (POP).
QASP/Progress Reports	4.7	Draft due to the government proposal. Final QASP due to the COR and CO 20 days after award. Subsequent reports due quarterly and/or as requested.
Invoices	4.5	Invoice should be submitted on a monthly basis to the COR and designated Finance Center for all services performed and no more than 30 days in the arrears of the last day of the POP.

5.1 GENERAL REPORT REQUIREMENTS

The Contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with ICE workstations (Windows XP and Microsoft Office Applications).

5.2 ACCEPTANCE CRITERIA

ICE will accept or reject deliverables within fifteen (15) business days after delivery. If rejected, the Contractor shall make corrections as specified and resubmit the deliverable for review and approval within five (5) business days provided however that contractor is not dependent upon a third party for performance. If the government does not reply within the specific timeframe than the deliverable shall be determined acceptable.

6.0 SECTION 508 COMPLIANCE

Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) as amended by P.L. 105-220 under Title IV (Rehabilitation Act Amendments of 1998) all Electronic and Information Technology (EIT) developed, procured, maintained and/or used under this contract shall be in compliance with the "Electronic and Information Technology Accessibility Standards" set forth by the Architectural and Transportation Barriers Compliance Board (also referred to as the "Access Board") in 36 CFR Part 1194. The complete text of Section 508 Standards can be accessed at http://www.access-board.gov/ or at http://www.section508.gov.

7.0 PRIVACY REQUIREMENTS

Limiting Access to Privacy Act and Other Sensitive Information
In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984), and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires contractor personnel to have access to information protected by the Privacy Act of 1974, the contractor is advised that the relevant DHS system of records notices (SORNs) applicable to this Privacy Act information may be found at https://www.dhs.gov/system-records-notices-sorns. Applicable SORNS of other agencies may be accessed through the agencies' websites or by searching GovInfo, available at https://www.govinfo.gov that replaced the FDsys website in December 2018. SORNs may be updated at any time.

Prohibition on Performing Work Outside a Government Facility/Network/Equipment
The Contractor shall perform all tasks on authorized Government networks, using Government-furnished IT and other equipment and/or Workplace as a Service (WaaS) if WaaS is authorized by the statement of work. Government information shall remain within the confines of authorized Government networks at all times. Except where telework is specifically authorized within this contract, the Contractor shall perform all tasks described in this document at authorized Government facilities; the Contractor is prohibited from performing these tasks at or removing Government-furnished information to any other facility; and Government information shall remain within the confines of authorized Government facilities at all times. Contractors may only access classified materials on government furnished equipment in authorized government owned facilities regardless of telework authorizations.

Prior Approval Required to Hire Subcontractors
The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (Subcontractor) in support of this contract requiring the disclosure of

information, documentary material and/or records generated under or relating to this contract. The Contractor (and any Subcontractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

Separation Checklist for Contractor Employees
Contractor shall complete a separation checklist before any employee or Subcontractor employee terminates working on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposal of sensitive personally identifiable information (PII), in paper or electronic form, in the custody of the employee or Subcontractor employee including the sanitization of data on any computer systems or media as appropriate; and (3) termination of any technological access to the Contractor's facilities or systems that would permit the terminated employee's access to sensitive PII.
In the event of adverse job actions resulting in the dismissal of an employee or Subcontractor employee, the Contractor shall notify the Contracting Officer's Representative (COR) within 24 hours. For normal separations, the Contractor shall submit the checklist on the last day of employment or work on the contract.

As requested, contractors shall assist the ICE Point of Contact (ICE/POC), Contracting Officer, or COR with completing ICE Form 50-005/Contractor Employee Separation Clearance Checklist by returning all Government-furnished property including but not limited to computer equipment, media, credentials and passports, smart cards, mobile devices, PIV cards, calling cards, and keys and terminating access to all user accounts and systems.

Contractor's Commercial License Agreement and Government Electronic Information Rights
Except as stated in the Performance Work Statement and, where applicable, the Contractor's Commercial License Agreement, the Government Agency owns the rights to all electronic information (electronic data, electronic information systems or electronic databases) and all supporting documentation and associated metadata created as part of this contract. All deliverables (including all data and records) under the contract are the property of the U.S. Government and are considered federal records, for which the Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

Privacy Lead Requirements
If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy documentation, the Contractor shall assign or procure a Privacy Lead, to be listed under the SOW or PWS's required Contractor Personnel section. The Privacy Lead shall be responsible for providing adequate support to DHS to ensure DHS can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance. The Privacy Lead shall work with personnel from the program office, the ICE Privacy Unit, the Office of the Chief Information Officer, and the Records and Data Management Unit to ensure that the privacy documentation is kept on schedule, that the answers to questions in the PIA are thorough and complete, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.

The Privacy Lead:

- Must have excellent writing skills, the ability to explain technology clearly for a non-technical audience, and the ability to synthesize information from a variety of sources.
- Must have excellent verbal communication and organizational skills.
- Must have experience writing PIAs. Ideally the candidate would have experience writing PIAs for DHS.
- Must be knowledgeable about the Privacy Act of 1974 and the E-Government Act of 2002.
- Must be able to work well with others.

If a Privacy Lead is already in place with the program office and the contract involves IT system builds or substantial changes that may require privacy documentation, the requirement for a separate Private Lead specifically assigned under this contract may be waived provided the Contractor agrees to have the existing Privacy Lead coordinate with and support the ICE Privacy POC to ensure privacy concerns are proactively reviewed and so ICE can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance if required. The Contractor shall work with personnel from the program office, the ICE Office of Information Governance and Privacy, and the Office of the Chief Information Officer to ensure that the privacy documentation is kept on schedule, that the answers to questions in any privacy documents are thorough and complete, that all records management requirements are met, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.

LexisNexis - Attachment 3-Price Matrix

Law Enforcement Investigative Database Subscription (LEIDS)

Pricing should be based on (b)(4)

Contract Line Item Number	Description	Quantity	Unit of Measure	Montly Price	Monthly Price if both tasks are awarded (this should include any discounts)
CLIN 0001 3/1/2021-2/28/2022	Database Functionality Requirements Task 1	12	Month	(b)(4)	N/A
CLIN 0002 3/1/2021-2/28/2022	Training and User Maintenance Task 1A	12	Month		N/A
CLIN 0003 3/1/2021-2/28/2022	LPR Task 2	12	Month		N/A
CLIN 0004 3/1/2021-2/28/2022	LPR Training and User Maintenance Task 2A	12	Month		N/A
CLIN 1001 3/1/2022-2/28/2023	Database Functionality Requirements Task 1	12	Month		N/A
CLIN 1002 3/1/2022-2/28/2023	Training and User Maintenance Task 1A	12	Month		N/A
CLIN 1003 3/1/2022-2/28/2023	LPR Task 2	12	Month		N/A
CLIN 1004 3/1/2022-2/28/2023	LPR Training and User Maintenance Task 2A	12	Month		N/A
CLIN 2001 3/1/2023-2/29/2024	Database Functionality Requirements Task 1	12	Month		N/A
CLIN 2002 3/1/2023-2/29/2024	Training and User Maintenance Task 1A	12	Month		N/A
CLIN 2003 3/1/2023-2/29/2024	LPR Task 2	12	Month		N/A
CLIN 2004 3/1/2023-2/29/2024	LPR Training and User Maintenance Task 2A	12	Month		N/A
CLIN 3001 3/1/2024-2/28/2025	Database Functionality Requirements Task 1	12	Month		N/A
CLIN 3002 3/1/2024-2/28/2025	Training and User Maintenance Task 1A	12	Month		N/A
CLIN 3003 3/1/2024-2/28/2025	LPR Task 2	12	Month		N/A
CLIN 3004 3/1/2024-2/28/2025	LPR Training and User Maintenance Task 2A	12	Month		N/A
CLIN 4001 3/1/2025-2/28/2026	Database Functionality Requirements Task 1	12	Month		N/A
CLIN 4002 3/1/2025-2/28/2026	Training and User Maintenance Task 1A	12	Month		N/A
CLIN 4003 3/1/2025-2/28/2026	LPR Task 2	12	Month		N/A
CLIN 4004 3/1/2025-2/28/2026	LPR Training and User Maintenance Task 2A	12	Month		N/A
TOTAL PRICE INCLUDING ALL OPTIONS				**$16,819,344**	N/A

Enterprise Architecture (EA) Compliance Language FY

This is a list of EA Architecture Compliance language agreed upon between Components and HQ DHS to be used in preparing SOW, PWS & SOO for IT acquisitions & services. The following Components (CBP, TSA & USCG) have their own customized version listed below that must be used. All other Components must use the DHS Enterprise Architecture Compliance language that follows:

DHS Enterprise Architecture Compliance

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following HLS EA requirements:

- All developed solutions and requirements shall be compliant with the HLS EA.
- All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
- Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Architecture Division (EAD) for review, approval and insertion into the DHS Data Reference Model and Mobius.
- Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.
- Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

U.S. Customs and Border Protection (CBP)

DHS-CBP Enterprise Architecture Compliance

The Offeror shall ensure that the design conforms to the Department of Homeland Security (DHS) and Customs and Border Protection (CBP) Enterprise Architecture (EA), the DHS and CBP Technical Reference Models (TRM), and all DHS and CBP policies and guidelines (such as the CBP Information Technology Enterprise Principles and the DHS Service Oriented Architecture - Technical Framework), as promulgated by the DHS and CBP Chief Information Officers (CIO), Chief Technology Officers (CTO) and Chief Architects (CA).

The Offeror shall conform to the Federal Enterprise Architecture (FEA) model and the DHS and CBP versions of the FEA model, as described in their respective EAs. All models will be submitted using Business Process Modeling Notation (BPMN 1.1 or BPMN 2.0 when available) and the CBP Architectural Modeling Standards. Universal Modeling Language (UML2) may be used for infrastructure only. Data semantics shall be in conformance with the National Information Exchange Model (NIEM). Development solutions will also ensure compliance with the current version of the DHS and CBP target architectures.

Where possible, the Offeror shall use DHS/CBP approved products, standards, services, and profiles, as reflected by the hardware, software, application, and infrastructure components of the DHS/CBP TRM/standards profile. If new hardware, software, or infrastructure components are required to develop, test, or implement the program, these products will be coordinated through the DHS and CBP formal Technology Insertion (TI) process (to include a trade study with no less than four alternatives, one of which reflecting the status quo and another reflecting multi-agency collaboration). The DHS/CBP TRM/standards profile will be updated as TIs are resolved.

All developed solutions shall be compliant with the Homeland Security (HLS) EA. All IT hardware and software shall be compliant with the HLS EA.

Compliance with the HLS EA shall be derived from and aligned through the CBP EA.

Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Architecture Division (EAD) for review, approval, and insertion into the DHS Data Reference Model and Mobius.

Development of data assets, information exchanges, and data standards will comply with the DHS Data Management Policy MD 103-01. All data-related artifacts will be developed and validated according to DHS Data Management Architectural Guidelines.

Applicability of Internet Protocol version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS EA (per OMB Memorandum M-05-22, August 2, 2005), regardless of whether the acquisition is for modification, upgrade, or replacement. All EA related component acquisitions shall be IPv6 compliant, as defined in the USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of conformance, defined in the USGv6 Test Program.

Transportation Security Administration

DHS-TSA Enterprise Architecture Compliance

a) The Contractor shall ensure that all architectural artifacts including but not limited to solutions, business, Data, IT elements for legacy Transportation Security Equipment (TSE), Information Systems Security Agreements (ISSAs), System Design documents (SDDs), deliverables, and services are aligned and compliant with the current DHS and TSA Enterprise Architecture, and the Federal Enterprise Architecture Framework (OMB Reference Models), the Technology Business Management (TBM) Taxonomy, and Federal Information Technology Acquisition Reform Act (FITARA).
   i. All solutions and services shall meet DHS and TSA Enterprise Architecture policies, standards, and procedures. Specifically:
      a. DHS and TSA Enterprise Architecture policies, standards, and procedures.
      b. Homeland Security Enterprise Architecture (HLS EA) and TSA EA requirements.
      c. TSA and DHS IT Security, Cloud, Infrastructure (including Network), Application/Systems, Information/Data, Performance, and Business Architecture policies, directives, guidelines, standards, segment architectures and reference architectures.
      d. TSA functional capabilities
      e. TSA operational capabilities
      f. TSA lines of business
      g. TSA business processes
      h. TSA funding sources
      i. TBM Taxonomy for IT cost transparency
   ii. This includes new Transportation Security Equipment (TSE) and Legacy TSE that utilizes IT software, services, or equipment including embedded IT elements such as network switches, routers, In printers, etc.
   iii. All solutions shall implement and leverage TSA information and data standards as defined and approved per TSA policy.
   iv. All solution architectures and services (e.g., Application, System, Network, Security, Information/Data, Cloud) shall be reviewed and approved by TSA EA as part of the TSA SELC (System Engineering Life Cycle) review process and in accordance with TSA IT Governance Management Directive 1400.20 with applicable DHS and TSA IT governance policies, directives, and processes. This includes the Solution Engineering Review (SER), Preliminary Design Review (PDR) and Critical Design Review (CDR) stage gates. The required design artifacts include solution approach document and System Design Document (SDDs) as directed by EAD, all implementations shall follow the approved solution architecture/design without deviation. Any changes, to either the prior approved solution and/or prior approved design that are identified during subsequent SELC phases, including testing, implementation and deployment, shall undergo additional EA review prior to proceeding.

v. TSA Offices acquiring Enterprise architecture type services at segment or solution levels shall engage and collaborate with the TSA Enterprise Architecture Division (EAD) to ensure strategic alignment of people, process, information, and technology and comply with enterprise level architecture governance, artifacts and standards.
    a. The Contractor shall engage domain architect(s) in EAD before SELC Obtain Phase, i.e. during SELC Need or "Analyze and Select" Phase.
    b. The Contractors shall collaborate with the EA domain architect(s) to deliver the required design artifacts and desired outcome under the guidance.
    c. The Contractor shall provide architecture and system/application data and models in prescribed formats to be stored in TSA's Enterprise Architecture Repository.

b) In accordance with the TSA Cloud Strategy 2.0, April 2019, TSA's approach to cloud computing and governance of migration to the cloud, the contractor shall ensure that the cloud solutions utilize the SaaS (Software as a Service) model as its primary approach to cloud implementation, and also, when necessary will use Platform as a Service (PaaS) or Infrastructure as a Service (IaaS). The contractor shall adhere to the principles of cloud strategy to systematically retire or replace legacy applications by use of an integrated approach to cloud planning, architecture, hybrid deployment, and operation.

c) Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

Information and Data Governance and Management

d) The Contractor shall develop, use, and dispose of TSA information and data assets following the TSA governance processes established by the Enterprise Information/Data Governance Board (EIDGB), in compliance with the DHS Enterprise Data Governance and Management MD (Management Directive) 103-01.
    i. TSA information and data assets include but are not limited to the TSA Data Catalog, TSA information and data standards, TSA Data Management Plan, TSA data sets (including open data sets for public consumption), TSA information and data stored in TSA repositories, TSA information and data in systems and applications (internal and external), and TSA information exchanges.
    ii. All TSA information and data, and all solutions that capture, store, use and provide TSA information and data shall comply with the Geospatial Data Act (GDA) of 2018 (P.L. 115-254) that requires agencies to foster efficient management of geospatial data/information, technologies, and infrastructure

through enhanced coordination among Federal, state, local, and tribal governments, along with private sector and academia.

iii. Description information for all data assets shall be submitted to the TSA Enterprise Architecture Team, who will be responsible for coordination with DHS, and for review, approval and insertion into the TSA Data Reference Model and Enterprise Architecture Repository.

iv. In addition to the Federal Acquisitions Regulations (FAR) Subpart 27.4 – 'Rights in Data and Copyrights' and Section 35.011 detailing technical data delivery, the contractor shall provide all TSA-specific data in a format maintaining pre-existing referential integrity and data constraints, as well as data structures in a format understandable to TSA. Examples of data structures can be defined as, but not limited to:

   a. Data models containing entities and attributes, identifying authoritative and trusted data sources, and depicting relationship mapping and, or linkages
   b. Metadata information to define data definitions
   c. Detailed data formats, type, and size
   d. Delineations of the referential integrity (e.g., primary key/foreign key) of data schemas, structures, and or taxonomies
   e. Information exchange specifications

v. All TSA-specific data shall be delivered in a secure and timely manner to TSA. Data security is defined within the 'Requirements for Handling Sensitive, Classified, and/or Proprietary Information', section of this SOW (Statement of Work), SOO (Statement of Objectives) and PWS (Performance Work Statement). This definition complies with not only the delivery of data, but also maintaining TSA-specific data within a non-TSA or DHS proprietary system.

vi. All metadata shall be pre-defined upon delivery to TSA. Metadata shall be delivered in a format that is readily interpretable by TSA (e.g., metadata shall be extracted from any metadata repository that is not utilized by TSA and delivered in a TSA approved manner). Metadata shall also provide an indication of historical version, the most current data to be used, as well as frequency of data refreshes.

vii. The contractor shall provide a Data Asset Repository Profile (DAR) and Data Management Plan (DMP) to EA using EA provided template before the preliminary/critical design review. The DAR and DMP include conceptual and logical data models, data dictionaries, data asset profile, and other artifacts pertinent to the project's data.

viii. TSA adheres to the DHS NIEM (National Information Exchange Model) First policy and standards outlined in the DHS Memorandum, "Adoption of the National Information Exchange Model within the Department of Homeland Security," dated May 3, 2019. All TSA information and data exchanges shall be NIEM compliant. All TSA solutions that leverage TSA information and data exchanges shall be NIEM compliant.

United States Coast Guard

DHS-USCG Enterprise Architecture Compliance

All solutions and services shall meet DHS and USCG Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following Homeland Security Enterprise Architecture (HLS EA) and USCG EA requirements:

- All developed solutions and requirements shall be compliant with the HLS and USCG EAs.
- All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile and with the USCG IT Products and Standards Inventory.
- Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to USCG Enterprise Architecture Division (EAD) and DHS Enterprise Architecture Division (EAD) for review, approval and insertion into the USCG and DHS Data Reference Model and Mobius.
- Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.
- Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

a. The Offeror understands and agrees that the Government retains the right to cancel or terminate the Contract, if the Government determines that continuing this solicitation presents an unacceptable risk to national security.

b. “Gray-Market” Equipment

   i. The Offeror shall provide only new equipment unless otherwise expressly approved, in writing, by the DHS Contracting Officer. Offerors shall provide only Original Equipment Manufacturer (OEM) parts to the Government. In the event that a shipped OEM part fails, all replacement parts must be OEM parts.

   ii. The Offeror shall be excused from using new OEM (i.e., "gray market”, "previously used”) components only with formal Government approval, in writing, from the DHS Contracting Officer. Such components shall be procured from their original source and shipped only from the manufacturer’s authorized shipment points.

   iii. All equipment obtained by the Offeror on behalf of the Government will need to be provided to OIG OCIO for review to validate requirements and approved Contractors by DHS.

c. Hardware and Software Requests

   i. The contractors supply the Government hardware and software will provide the manufacturer’s name, address, state, and/or domain of registration, and the DUNS number for all components comprising the hardware and software. If subcontractors or subcomponents are used, the name, address, state, and/or domain of registration and DUNS number of those suppliers must be provided.

   ii. Subcontractors are subject to the same general requirements and standards as prime contractors. Contractors employing subcontractors will perform due diligence to ensure that these standards are met.

   iii. The Government shall be notified when a new contractor/subcontractor/service provider is introduced to the supply chain, or when suppliers of parts or subcomponents are changed.

      1. For software products, the Offeror shall provide all OEM software updates to correct defects for the life of the product (i.e., until the “End of Life (EoL)"). Software updates and patches shall be either: made available to the government for all products procured under this Contract, replaced upon End of Support (EoS) is reached, or formally waived (in writing) by the DHS Contracting Officer.

d. Supply-Chain Transport

   i. Offerors shall employ formal and accountable transit, storage, and delivery procedures (i.e., the possession of the component is documented at all times from initial shipping point to final destination, and every transfer of the component from one custodian to another is fully documented and accountable) for all shipments to fulfill Contract obligations with the Government.

   ii. All records pertaining to the transit, storage, and delivery will be maintained and available for inspection for the lessor of the term of the

Contract, the period of performance, or one calendar year from the date the activity occurred.

iii. This transit process shall minimize the number of times in route components undergo a change of custody and make use of tamper-proof or tamper-evident packaging for all shipments. The supplier, at the Government's request, shall be able to provide shipping status at any time during transit.

iv. All records pertaining to the transit, storage, and delivery shall be readily available for inspection by any agent designated by the U.S. Government as having the authority to examine them.

v. The Offeror is fully liable for all damage, deterioration, or losses incurred during shipping and handling, unless the damage, deterioration, or loss is due to the Government.

vi. The Offeror shall provide a packing slip which shall accompany each container or package with the information identifying this solicitation number, the order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact.

vii. The Offeror shall send a shipping notification to the intended government recipient; with a copy transmitted via email to the Contracting Officer, or designated representative. This shipping notification shall be sent electronically and will state this solicitation number, the order number, a description of the hardware/software being ship (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

e. Notifications

i. The Offeror shall notify DHS Contracting Officer, COR and the Office of the Chief Information Officer and the DHS component Chief Information Officer through the Enterprise Security Operations Center (ESOC) directly of any suspected or potential violations of Section 889 of the National Defense Authorization Act (NDAA) for Information Communications Technology (ICT) at NDAA_Incidents@hq.dhs.gov.

f. Foreign Equities

The Offeror shall immediately notify the DHS Contracting Officer, COR that will report to the Office of the Chief Security Officer (OCSO) or cognizant component personnel security office regarding any changes to corporate foreign ownership, control, or influence.

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS

OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER	PAGE	OF
192121FLMURQ0010	1	5

2. CONTRACT NO.	3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
70CMSD21C00000001	2/25/2021		70CMSD21R00000002	01/20/2021

7. FOR SOLICITATION INFORMATION CALL:

a. NAME: (b)(6); (b)(7)(C)

b. TELEPHONE NUMBER (No collect calls): 214-905 (b)(6); (b)(7)(C)

8. OFFER DUE DATE/LOCAL TIME: CT

9. ISSUED BY CODE: 70CMSD

INVESTIGATIONS & OPS SUPPORT DALLAS
U.S. Immigration and Customs Enforcement
Office of Acquisition Management
8222 N. BELTLINE ROAD, (b)(6); (b)(7)(C)
IRVING TX 75063

10. THIS ACQUISITION IS [X] UNRESTRICTED OR [ ] SET ASIDE: % FOR:

- [ ] SMALL BUSINESS
- [ ] HUBZONE SMALL BUSINESS
- [ ] SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
- [ ] WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
- [ ] EDWOSB
- [ ] 8(A)

NAICS: 519130

SIZE STANDARD: 500

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED	12. DISCOUNT TERMS	13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING	14. METHOD OF SOLICITATION
[ ] SEE SCHEDULE	Net 30	[ ]		[ ] RFQ [ ] IFB [X] RFP

15. DELIVER TO CODE: ICE/HSI/HQ-D5

ICE Hmlnd Sec Inv HQ (b)(6); (b)(7)(C)
Immigration and Customs Enforcement
500 12th Street SW
Washington DC 20024

16. ADMINISTERED BY CODE: ICE/IOSD

Investigations Ops Support Dallas
Immigration and Customs Enforcement
Office of Acquisition Management
7701 N. Stemmons Freeway, (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Dallas TX 75247

17a. CONTRACTOR/ OFFEROR CODE: 060117244 FACILITY CODE:

LEXISNEXIS RISK SOLUTIONS INC
ATTN (b)(6); (b)(7)(C)
1000 ALDERMAN DR
ALPHARETTA GA 300054101

TELEPHONE NO. (b)(6); (b)(7)(C)

[ ] 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18a. PAYMENT WILL BE MADE BY CODE: ICE-HSI-HQ-DIV 5

DHS, ICE
Burlington Finance Center
P.O. Box 1620
Attn: (b)(6); (b)(7)(C)
Williston VT 05495-1620

[ ] 18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED [ ] SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	DUNS Number: 060117244 (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) This contract establishes the purchase of Law Enforcement Investigative Database Services *(Use Reverse and/or Attach Additional Sheets as Necessary)*				

25. ACCOUNTING AND APPROPRIATION DATA: See schedule

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*: $3,168,000.00

[ ] 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED.

[X] 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4, FAR 52.212-5 IS ATTACHED. ADDENDA [X] ARE [ ] ARE NOT ATTACHED.

[X] 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.

[ ] 29. AWARD OF CONTRACT: _____ OFFER DATED _____. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR	31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*
	(b)(6); (b)(7)(C)

30b. NAME AND TITLE OF SIGNER *(Type or print)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(Type or print)*	31c. DATE SIGNED
		(b)(6); (b)(7)(C)	2/25/201

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	(LEIDS) in accordance with the Performance Work Statement (PWS) and the Contract Line Item Numbers (CLINs) contained in this contract. Attachments applicable to this contract are: Attachment 1-Clauses Attachment 2-PWS (dated December 10, 2020) Attachment 3-Price Matrix Attachment 4-All AE Compliance Language (2021) Attachment 5-C-SCRM Language ~ Period of Performance: 03/01/2021 to 02/28/2022				
0001	LAW ENFORCEMENT INVESTIGATIVE DATABASE SUBSCRIPTION Task 1-Database functionality requirements Task 1A-Training and User Maintenance POP 3/1/21-2/28/22 Accounting Info: (b)(7)(E) ------ --- Funded: $1,524,170.16 Accounting Info: (b)(7)(E) ------ --- Funded: $1,524,170.16 Accounting Info: Continued ...	(b)(4)			3,168,000.00

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE
	32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT	37. CHECK NUMBER
☐ PARTIAL ☐ FINAL			☐ COMPLETE ☐ PARTIAL ☐ FINAL	

38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(Print)*	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT *(Location)*	
		42c. DATE REC'D *(YY/MM/DD)*	42d. TOTAL CONTAINERS

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	(b)(7)(E) ---- ---				
	Funded: $119,659.68				
1001	LAW ENFORCEMENT INVESTIGATIVE DATABASE SUBSCRIPTION Task 1-Database functionality requirements Task 1A-Training and User Maintenance POP 3/1/22-2/28/23 Amount: $3,263,040.00(Option Line Item) 02/28/2022			(b)(4)	0.00
2001	LAW ENFORCEMENT INVESTIGATIVE DATABASE SUBSCRIPTION Task 1-Database functionality requirements Task 1A-Training and User Maintenance POP 3/1/23-2/29/24 Amount: $3,360,936.00(Option Line Item) 02/28/2023			(b)(4)	0.00
3001	LAW ENFORCEMENT INVESTIGATIVE DATABASE SUBSCRIPTION Task 1-Database functionality requirements Task 1A-Training and User Maintenance POP 3/1/24-2/28/25 Amount: $3,461,760.00(Option Line Item) 02/29/2024			(b)(4)	0.00
4001	LAW ENFORCEMENT INVESTIGATIVE DATABASE SUBSCRIPTION Task 1-Database functionality requirements Task 1A-Training and User Maintenance POP 3/1/25-2/28/26 Amount: $3,565,608.00(Option Line Item) 02/28/2025			(b)(4)	0.00
	INVOICE INSTRUCTIONS 1. The contractor shall be active in the System for Award Management (www.SAM.gov) for invoice processing. Besides the information identified below, a proper invoice shall also include; contractor's Dunn and Bradstreet (D&B) DUNS Continued ...				

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)

number; the ICE Program Office; and state whether the invoice is "INTERIM" or "FINAL".

2. In accordance with Contract Clauses, FAR 52.212-4 (g) (1), Contract Terms and Conditions - Commercial Items, or FAR 52.232-25 (a) (3), Prompt Payment, as applicable, the information required with each invoice submission is as follows:

"...An invoice must include-

(i) Name and address of the Contractor. The name, address and DUNS number on the invoice MUST match the information in both the Contract/Agreement and the information in SAM;

(ii) Dunn and Bradstreet (D&B) DUNS number;

(iii) Invoice date and number;

(iv) Contract number, line items and, if applicable, the order number;

(v) Description, quantity, unit of measure, unit price and extended price of the items delivered;

(vi) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading;

(vii) Terms of any discount for prompt payment offered;

(viii) Remit to Address;

(ix) Name, title, and phone number of person to notify in event of defective invoice;

(x) ICE Program Office designated on the order/contract/agreement; and

(xi) Whether the invoice is "Interim" or "Final"

3. Invoice submission: shall be submitted via one of the following two methods. Improper invoices or those submitted by means other than these two methods will be returned. Email is the preferred method.

a. Primary method of submission is email. The Contractor shall submit one (1) invoice in PDF format per e-mail and the subject line of the e-mail will reference the invoice number of the attached invoice to:
Invoice.Consolidation@ice.dhs.gov
Attn: ICE - (Insert program office name or code) Invoice

Continued ...

NAME OF OFFEROR OR CONTRACTOR
LEXISNEXIS RISK SOLUTIONS INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)

b. Mail:
DHS, ICE
Financial Service Center Burlington
Attn: ICE-_____ Invoice
(Insert program office name or code)
P.O. Box 1620
Williston, VT 05495-1620

4. Payment Inquiries: Questions regarding invoice submission or payment, please contact Financial Service Center Burlington at 1-877-491-6521, Option # 3 or by e-mail at OCFO.CustomerService@ice.dhs.gov

Invoices without the above information may be returned for resubmission.

The total amount of award: $16,819,344.00. The obligation for this award is shown in box 26.

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS

OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER	PAGE	OF
192121FLMURQ0010	1	5

2. CONTRACT NO.	3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
70CMSD21C00000001	2/25/2021		70CMSD21R0000002	01/20/2021

7. FOR SOLICITATION INFORMATION CALL:

a. NAME: (b)(6); (b)(7)(C)

b. TELEPHONE NUMBER (No collect calls): 214-905-(b)(6); (b)(7)(C)

8. OFFER DUE DATE/LOCAL TIME: CT

9. ISSUED BY CODE: 70CMSD

INVESTIGATIONS & OPS SUPPORT DALLAS
U.S. Immigration and Customs Enforcement
Office of Acquisition Management
8222 N. BELTLINE ROAD, (b)(6); (b)(7)(C)
IRVING TX 75063

10. THIS ACQUISITION IS [X] UNRESTRICTED OR [ ] SET ASIDE: % FOR:

- [ ] SMALL BUSINESS
- [ ] HUBZONE SMALL BUSINESS
- [ ] SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
- [ ] WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
- [ ] EDWOSB
- [ ] 8(A)

NAICS: 519130

SIZE STANDARD: 500

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED
[ ] SEE SCHEDULE

12. DISCOUNT TERMS
Net 30

[ ] **13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)**

13b. RATING

14. METHOD OF SOLICITATION
[ ] RFQ [ ] IFB [X] RFP

15. DELIVER TO CODE: ICE/HSI/HQ-D5

ICE Hmlnd Sec Inv HQ (b)(6); (b)(7)(C)
Immigration and Customs Enforcement
500 12th Street SW
Washington DC 20024

16. ADMINISTERED BY CODE: ICE/IOSD

Investigations Ops Support Dallas
Immigration and Customs Enforcement
Office of Acquisition Management
7701 N. Stemmons Freeway, (b)(6); (b)(7)(C)
Attn: (b)(6); (b)(7)(C)
Dallas TX 75247

17a. CONTRACTOR/ OFFEROR CODE: 060117244000 FACILITY CODE:

LEXISNEXIS RISK SOLUTIONS INC
ATTN (b)(6); (b)(7)(C)
1000 ALDERMAN DR
ALPHARETTA GA 300054101

TELEPHONE NO. (b)(6); (b)(7)(C)

[ ] **17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER**

18a. PAYMENT WILL BE MADE BY CODE: ICE-HSI-HQ-DIV 5

DHS, ICE
Burlington Finance Center
P.O. Box 1620
Attn: ICE-HSI-HQ-Div 5
Williston VT 05495-1620

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED [ ] SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	DUNS Number: 060117244 (b)(6); (b)(7)(C) This contract establishes the purchase of Law Enforcement Investigative Database Services *(Use Reverse and/or Attach Additional Sheets as Necessary)*				

25. ACCOUNTING AND APPROPRIATION DATA
See schedule

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*
$3,168,000.00

[ ] 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4, FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED.

[X] 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA [X] ARE [ ] ARE NOT ATTACHED.

[X] **28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN** 1 **COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.**

[ ] **29. AWARD OF CONTRACT:** _____ OFFER DATED _____. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR

31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*
(b)(6); (b)(7)(C)

30b. NAME AND TITLE OF SIGNER *(Type or print)*

30c. DATE SIGNED

31b. NAME OF CONTRACTING OFFICER *(Type or print)*
(b)(6); (b)(7)(C)

31c. DATE SIGNED
2/25/201

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	(LEIDS) in accordance with the Performance Work Statement (PWS) and the Contract Line Item Numbers (CLINs) contained in this contract. Attachments applicable to this contract are: Attachment 1-Clauses Attachment 2-PWS (dated December 10, 2020) Attachment 3-Price Matrix Attachment 4-All AE Compliance Language (2021) Attachment 5-C-SCRM Language ~ Period of Performance: 03/01/2021 to 02/28/2022				
0001	LAW ENFORCEMENT INVESTIGATIVE DATABASE SUBSCRIPTION Task 1-Database functionality requirements Task 1A-Training and User Maintenance POP 3/1/21-2/28/22 Accounting Info: (b)(7)(E) ------ --- Funded: $1,524,170.16 Accounting Info: (b)(7)(E) ------ --- Funded: $1,524,170.16 Accounting Info: Continued ...	(b)(4)			3,168,000.00

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE 32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER ☐ PARTIAL ☐ FINAL	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT ☐ COMPLETE ☐ PARTIAL ☐ FINAL	37. CHECK NUMBER

38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(Print)*	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT *(Location)*	
		42c. DATE REC'D *(YY/MM/DD)*	42d. TOTAL CONTAINERS

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	(b)(7)(E) ---- --- Funded: $119,659.68				
1001	LAW ENFORCEMENT INVESTIGATIVE DATABASE SUBSCRIPTION Task 1-Database functionality requirements Task 1A-Training and User Maintenance POP 3/1/22-2/28/23 Amount: $3,263,040.00(Option Line Item) 02/28/2022			(b)(4)	0.00
2001	LAW ENFORCEMENT INVESTIGATIVE DATABASE SUBSCRIPTION Task 1-Database functionality requirements Task 1A-Training and User Maintenance POP 3/1/23-2/29/24 Amount: $3,360,936.00(Option Line Item) 02/28/2023			(b)(4)	0.00
3001	LAW ENFORCEMENT INVESTIGATIVE DATABASE SUBSCRIPTION Task 1-Database functionality requirements Task 1A-Training and User Maintenance POP 3/1/24-2/28/25 Amount: $3,461,760.00(Option Line Item) 02/29/2024			(b)(4)	0.00
4001	LAW ENFORCEMENT INVESTIGATIVE DATABASE SUBSCRIPTION Task 1-Database functionality requirements Task 1A-Training and User Maintenance POP 3/1/25-2/28/26 Amount: $3,565,608.00(Option Line Item) 02/28/2025			(b)(4)	0.00
	INVOICE INSTRUCTIONS 1. The contractor shall be active in the System for Award Management (www.SAM.gov) for invoice processing. Besides the information identified below, a proper invoice shall also include; contractor's Dunn and Bradstreet (D&B) DUNS Continued ...				

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)

number; the ICE Program Office; and state whether the invoice is "INTERIM" or "FINAL".

2. In accordance with Contract Clauses, FAR 52.212-4 (g) (1), Contract Terms and Conditions - Commercial Items, or FAR 52.232-25 (a) (3), Prompt Payment, as applicable, the information required with each invoice submission is as follows:

"...An invoice must include-

(i) Name and address of the Contractor. The name, address and DUNS number on the invoice MUST match the information in both the Contract/Agreement and the information in SAM;

(ii) Dunn and Bradstreet (D&B) DUNS number;

(iii) Invoice date and number;

(iv) Contract number, line items and, if applicable, the order number;

(v) Description, quantity, unit of measure, unit price and extended price of the items delivered;

(vi) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading;

(vii) Terms of any discount for prompt payment offered;

(viii) Remit to Address;

(ix) Name, title, and phone number of person to notify in event of defective invoice;

(x) ICE Program Office designated on the order/contract/agreement; and

(xi) Whether the invoice is "Interim" or "Final"

3. Invoice submission: shall be submitted via one of the following two methods. Improper invoices or those submitted by means other than these two methods will be returned. Email is the preferred method.

a. Primary method of submission is email. The Contractor shall submit one (1) invoice in PDF format per e-mail and the subject line of the e-mail will reference the invoice number of the attached invoice to:

Invoice.Consolidation@ice.dhs.gov

Attn: ICE - (Insert program office name or code) Invoice

Continued ...

NAME OF OFFEROR OR CONTRACTOR
LEXISNEXIS RISK SOLUTIONS INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	b. Mail: DHS, ICE Financial Service Center Burlington Attn: ICE-_____ Invoice (Insert program office name or code) P.O. Box 1620 Williston, VT 05495-1620 4. Payment Inquiries: Questions regarding invoice submission or payment, please contact Financial Service Center Burlington at 1-877-491-6521, Option # 3 or by e-mail at OCFO.CustomerService@ice.dhs.gov Invoices without the above information may be returned for resubmission. The total amount of award: $16,819,344.00. The obligation for this award is shown in box 26.				

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE OF PAGES
	1 3

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. *(If applicable)*
P00001	See Block 16C	192121FLMURQ0016	

6. ISSUED BY	CODE	7. ADMINISTERED BY *(If other than Item 6)*	CODE
70CMSD		ICE/IOSD	

INVESTIGATIONS & OPS SUPPORT DALLAS
U.S. Immigration and Customs Enforcement
Office of Acquisition Management
8222 N. BELTLINE ROAD, (b)(6); (b)(7)(C)
IRVING TX 75063

Investigations Ops Support Dallas
Immigration and Customs Enforcement
Office of Acquisition Management
7701 N. Stemmons Freeway, (b)(6); (b)(7)(C)
Attn: (b)(6); (b)(7)(C)
Dallas TX 75247

8. NAME AND ADDRESS OF CONTRACTOR *(No., street, county, State and ZIP Code)*

LEXISNEXIS RISK SOLUTIONS INC
ATTN (b)(6); (b)(7)(C)
1000 ALDERMAN DR
ALPHARETTA GA 300054101

(b)(6); (b)(7)(C)
3/5/21
LNRS Legal

CODE	FACILITY CODE
0601172440000	

(x) 9A. AMENDMENT OF SOLICITATION NO.

9B. DATED *(SEE ITEM 11)*

x 10A. MODIFICATION OF CONTRACT/ORDER NO. 70CMSD21C00000001

10B. DATED *(SEE ITEM 13)* 02/25/2021

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended. ☐ is not extended.
Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended , by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted ; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER If by virtue of this amendment you desire to change an offer already submitted , such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA *(If required)*
See Schedule

Net Increase: $112,500.00

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	
	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: *(Specify authority)* THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES *(such as changes in paying office, appropriation date, etc.)* SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
X	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: FAR 52.212-4 (c) changes
	D. OTHER *(Specify type of modification and authority)*

E. IMPORTANT: Contractor ☐ is not. ☒ is required to sign this document and return 1 copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION *(Organized by UCF section headings, including solicitation/contract subject matter where feasible.)*

DUNS Number: 060117244
Primary COR/Invoicing POC: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Alternate COR/Invoicing POC: (b)(6); (b)(7)(C)
Acquisition POC: (b)(6); (b)(7)(C)

The purpose of this modification is to update the Performance Work Statement (PWS) to include the penlink connector. The PWS dated December 10, 2020 is hereby replaced in its entirety with PWS dated March 5, 2021. As a result of this addition the Contract Line Items (CLINs) are affected as follows:
CLIN 0001 is increased by (b)(4)
Continued ...

Except as provided herein, all terms and conditions of the document referenced in Item 9 A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER *(Type or print)*	16A. NAME AND TITLE OF CONTRACTING OFFICER *(Type or print)*
(b)(6); (b)(7)(C) CEO (LNSSI)	(b)(6); (b)(7)(C)

15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
(b)(6); (b)(7)(C)	3/5/21	(b)(6); (b)(7)(C)	
(Signature of person authorized to sign)		*(Signature of Contracting Officer)*	

NAME OF OFFEROR OR CONTRACTOR
LEXISNEXIS RISK SOLUTIONS INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	CLIN 1001 is increased by (b)(4) from (b)(4) CLIN 2001 is increased by (b)(4) from (b)(4) CLIN 3001 is increased by (b)(4) from (b)(4) CLIN 4001 is increased by (b)(4) from (b)(4) The total obligated amount on this contract is increased (b)(4) to (b)(4) The total contract value is increased by $562,500.00 from $16,819,344.00 to $17,381,844.00. All other terms and conditions remain the same. ~ Period of Performance: 03/01/2021 to 02/28/2022 Change Item 0001 to read as follows(amount shown is the obligated amount):				
0001	LAW ENFORCEMENT INVESTIGATIVE DATABASE SUBSCRIPTION Task 1-Database functionality requirements Task 1A-Training and User Maintenance POP 3/1/21-2/28/22 Accounting Info: (b)(7)(E) ------ --- Funded: $0.00 Accounting Info: (b)(7)(E) ------ --- Funded: $0.00 Accounting Info: (b)(7)(E) --- --- Funded: $0.00 Accounting Info: (b)(7)(E) Funded: $112,500.00				(b)(4)
	Change Item 1001 to read as follows(amount shown is the obligated amount): Continued ...				

NAME OF OFFEROR OR CONTRACTOR
LEXISNEXIS RISK SOLUTIONS INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
1001	LAW ENFORCEMENT INVESTIGATIVE DATABASE SUBSCRIPTION Task 1-Database functionality requirements Task 1A-Training and User Maintenance POP 3/1/22-2/28/23 Amount: $3,375,540.00(Option Line Item) 02/28/2022				0.00
	Change Item 2001 to read as follows(amount shown is the obligated amount):				
2001	LAW ENFORCEMENT INVESTIGATIVE DATABASE SUBSCRIPTION Task 1-Database functionality requirements Task 1A-Training and User Maintenance POP 3/1/23-2/29/24 Amount: $3,473,436.00(Option Line Item) 02/28/2023				0.00
	Change Item 3001 to read as follows(amount shown is the obligated amount):				
3001	LAW ENFORCEMENT INVESTIGATIVE DATABASE SUBSCRIPTION Task 1-Database functionality requirements Task 1A-Training and User Maintenance POP 3/1/24-2/28/25 Amount: $3,574,260.00(Option Line Item) 02/29/2024				0.00
	Change Item 4001 to read as follows(amount shown is the obligated amount):				
4001	LAW ENFORCEMENT INVESTIGATIVE DATABASE SUBSCRIPTION Task 1-Database functionality requirements Task 1A-Training and User Maintenance POP 3/1/25-2/28/26 Amount: $3,678,108.00(Option Line Item) 02/28/2025				0.00

The following FAR and HSAR clauses will be included in the resulting contract. The clauses are updated as of FAC 2020-09 Effective 26 October 2020

FAR 52.212-4 Contract Terms and Conditions - Commercial Items. (Oct 2018)

FAR 52.212-5 -- Contract Terms and Conditions Required to Implement Statutes or Executive Orders -- Commercial Items (Oct 2020) (Deviation Apr 2020)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(2) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).

(3) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Aug 2019) (Section 889(a)(1)(A) of Pub. L. 115-232).

(4) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015)

(5) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).

(6) 52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004) (Public Laws 108-77, 108-78 (19 U.S.C. 3805 note)).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the contracting officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

[Contracting Officer check as appropriate.]

X (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Jun 2020), with Alternate I (Oct 1995) (41 U.S.C. 4704 and 10 U.S.C. 2402).

X (2) 52.203-13, Contractor Code of Business Ethics and Conduct (Jun 2020) (41 U.S.C. 3509).

_ (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (Jun 2010) (Section 1553 of Pub L. 111-5) (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009).

X (4) 52.204-10, Reporting Executive compensation and First-Tier Subcontract Awards (Jun 2020) (Pub. L. 109-282) (31 U.S.C. 6101 note).

_ (5) [Reserved]

X (6) 52.204-14, Service Contract Reporting Requirements (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

_ (7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

X (8) 52.209-6, Protecting the Government' Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (Jun 2020) (31 U.S.C. 6101 note).

X (9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Oct 2018) (41 U.S.C. 2313).

_ (10) [Reserved]

_ (11)(i) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (Mar 2020) (15 U.S.C. 657a).

_ (ii) Alternate I (Mar 2020) of 52.219-3.

_ (12) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Mar 2020) (if the offeror elects to waive the preference, it shall so indicate in its offer)(15 U.S.C. 657a).

_ (ii) Alternate I (Mar 2020) of 52.219-4.

_ (13) [Reserved]

_ (14) (i) 52.219-6, Notice of Total Small Business Aside (Mar 2020) (15 U.S.C. 644).

_ (ii) Alternate I (Mar 2020) of 52.219-6.

_ (15) (i) 52.219-7, Notice of Partial Small Business Set-Aside (Mar 2020) (15 U.S.C. 644).

_ (ii) Alternate I (Mar 2020) of 52.219-7.

X (16) 52.219-8, Utilization of Small Business Concerns (Oct 2018) (15 U.S.C. 637(d)(2) and (3)).

X (17) (i) 52.219-9, Small Business Subcontracting Plan (Jun 2020) (15 U.S.C. 637 (d)(4))

_ (ii) Alternate I (Nov 2016) of 52.219-9.

X (iii) Alternate II (Nov 2016) of 52.219-9.

_ (iv) Alternate III (Nov 2016) of 52.219-9.

_ (v) Alternate IV (June 2020) of 52.219-9.

_ (18)(i) 52.219-13, Notice of Set-Aside of Orders (Mar 2020) (15 U.S.C. 644(r)).

_(ii) Alternate I (Mar 2020) of 52.219-13

_ (19) 52.219-14, Limitations on Subcontracting (Mar 2020) (15 U.S.C. 637(a)(14)).

X (20) 52.219-16, Liquidated Damages—Subcontracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).

_ (21) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (Mar 2020) (15 U.S.C. 657f).

X (22)(i) 52.219-28, Post Award Small Business Program Rerepresentation (May 2020) (15 U.S.C. 632(a)(2)).

_(ii) Alternate I (Mar 2020) of 52.219-28

_ (23) 52.219-29, Notice of Set-Aside for, or Sole Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (Mar 2020) (15 U.S.C. 637(m)).

_ (24) 52.219-30, Notice of Set-Aside for, or Sole Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (Mar 2020) (15 U.S.C. 637(m)).

_ (25) 52.219-32, Orders Issued Directly Under Small Business Reserves (Mar 2020) (15 U.S.C. 644(r)).

_ (26) 52.219-33, Nonmanufacturer Rule (Mar 2020) (15 U.S.C. 637(a)(17)).

X (27) 52.222-3, Convict Labor (June 2003) (E.O. 11755).

X (28) 52.222-19, Child Labor—Cooperation with Authorities and Remedies (Jun 2020) (E.O. 13126).

X (29) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

X (30)(i) 52.222-26, Equal Opportunity (Sep 2016) (E.O. 11246).

_ (ii) Alternate I (Feb 1999) of 52.222-26

X (31) 52.222-35, Equal Opportunity for Veterans (Jun 2020) (38 U.S.C. 4212).

_ (ii) Alternate I (July 2014) of 52.222-35

X (32) 52.222-36, Equal Opportunity for Workers with Disabilities (Jun 2020) (29 U.S.C. 793).

_ Alternate I (July 2014) of 52.222-36

X (33) 52.222-37, Employment Reports on Veterans (Jun 2020) (38 U.S.C. 4212).

X (34) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).

X (35) (i) 52.222-50, Combating Trafficking in Persons (Oct 2020) (22 U.S.C. chapter 78 and E.O. 13627).

_ (ii) Alternate I (Mar 2015) of 52.222-50, (22 U.S.C. chapter 78 and E.O. 13627).

_ (36) 52.222-54, Employment Eligibility Verification (Oct 2015). (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)

_ (37)(i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008) (42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

_ (ii) Alternate I (May 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

_ (38) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (Jun 2016) (E.O.13693).

_ (39) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (Jun 2016) (E.O. 13693).

_ (40) (i) 52.223-13, Acquisition of EPEAT® -Registered Imaging Equipment (Jun 2014) (E.O.s 13423 and 13514).

_ (ii) Alternate I (Oct 2015) of 52.223-13.

_ (41) (i) 52.223-14, Acquisition of EPEAT® -Registered Television (Jun 2014) (E.O.s 13423 and 13514).

_ (ii) Alternate I (Jun 2014) of 52.223-14.

_(42) 52.223-15, Energy Efficiency in Energy-Consuming Products (May 2020) (42 U.S.C. 8259b).

_ (43) 52.223-16, Acquisition of EPEAT® -Registered Personal Computer Products (Oct 2015) (E.O.s 13423 and 13514)

_ (ii) Alternate I (Jun 2014) of 52.223-16.

X (44) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging while Driving (Jun 2020) (E.O. 13513).

_ (45) 52.223.20, Aerosols (Jun 2016) (E.O. 13693).

_ (46) 52.223.21, Foams (Jun 2016) (E.O. 13696).

X (47) (i) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).

X (ii) Alternate I (Jan 2017) of 52.224-3.

_ (48) 52.225-1, Buy American Act--Supplies (May 2014) (41 U.S.C. chapter 83).

_ (49) (i) 52.225-3, Buy American Act--Free Trade Agreements--Israeli Trade Act (May 2014) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43).

_ (ii) Alternate I (May 2014) of 52.225-3.

_ (iii) Alternate II (May 2014) of 52.225-3.

_ (iv) Alternate III (May 2014) of 52.225-3.

_ (50) 52.225-5, Trade Agreements (Oct 2019) (19 U.S.C. 2501, *et seq.*, 19 U.S.C. 3301 note).

X (51) 52.225-13, Restrictions on Certain Foreign Purchases (Jun 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

_ (52) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2303 Note).

_ (53) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).

_ (54) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).

_ (55) 52.229-12, Tax on Certain Foreign Procurements (Jun 2020)

_ (56) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).

_ (57) 52.232-30, Installment Payments for Commercial Items (Jan 2017) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).

X (58) 52.232-33, Payment by Electronic Funds Transfer— System for Award Management (Oct 2018) (31 U.S.C. 3332).

_ (59) 52.232-34, Payment by Electronic Funds Transfer— Other Than System for Award Management (Jul 2013) (31 U.S.C. 3332).

_ (60) 52.232-36, Payment by Third Party (May 2014) (31 U.S.C. 3332).

X (61) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).

X (62) 52.242-5, Payments to Small Business Subcontractors (Jan 2017) (15 U.S.C. 637(d)(12)).

_ (63) (i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631).

_ (ii) Alternate I (Apr 2003) of 52.247-64.

_ (iii) Alternate II (Feb 2006) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or executive orders applicable to acquisitions of commercial items:

[*Contracting Officer check as appropriate.*]

_ (1) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67.).

_ (2) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

_ (3) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards -- Price Adjustment (Multiple Year and Option Contracts) (Aug 2018) (29 U.S.C.206 and 41 U.S.C. chapter 67).

_ (4) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards -- Price Adjustment (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

_ (5) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (May 2014) (41 U.S.C. chapter 67).

_ (6) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67).

_ (7) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015)

_ (8) 52.222-62, Paid Sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).

_ (9) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (May 2014) (42 U.S.C. 1792).

(d) *Comptroller General Examination of Record* The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records -- Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e) (1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c) and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause—

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509).

(ii) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(iii) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).

(iv) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Aug 2020) (Section 889(a)(1)(A) of Pub. L. 115-232).

(v) 52.219-8, Utilization of Small Business Concerns (Nov 2016) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $700,000 ($1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(vi) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

(vii) 52.222-26, Equal Opportunity (Sep 2016) (E.O. 11246).

(viii) 52.222-35, Equal Opportunity for Veterans (Oct 2015) (38 U.S.C. 4212).

(ix) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C. 793).

(x) 52.222-37, Employment Reports on Veterans (Feb 2016) (38 U.S.C. 4212).

(xi) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(xii) 52.222-41, Service Contract Labor Standards (Aug 2018), (41 U.S.C. chapter 67).

(xiii) (A) 52.222-50, Combating Trafficking in Persons (Jan 2019) (22 U.S.C. chapter 78 and E.O. 13627).

(B) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 E.O. 13627).

(xiv) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (May 2014) (41 U.S.C. chapter 67.)

(xv) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67)

(xvi) 52.222-54, Employment Eligibility Verification (Oct 2015) (E. O. 12989).

(xvii) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015).

(xviii) 52.222-62, Paid sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).

(xix) (A) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).

(B) Alternate I (Jan 2017) of 52.224-3.

(xx) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

(xxi) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (May 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xxii) 52.247-64, Preference for Privately-Owned U.S. Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64

(2) While not required, the contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of Clause)

Additional FAR Clauses incorporated by Reference:

FAR 52.204-13 System for Award Management Maintenance (Oct 2018)

FAR Clauses incorporated by Full Text:

52.203-17 Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights. (Jun 2020)

(a) This contract and employees working on this contract will be subject to the whistleblower rights and remedies in the pilot program on Contractor employee whistleblower protections established at 41 U.S.C. 4712 by section 828 of the National Defense Authorization Act for Fiscal Year 2013 (Pub. L. 112-239) and FAR 3.908.

(b) The Contractor shall inform its employees in writing, in the predominant language of the workforce, of employee whistleblower rights and protections under 41 U.S.C. 4712, as described in section FAR 3.908.

(c) The Contractor shall insert the substance of this clause, including this paragraph (c), in all subcontracts over the simplified acquisition threshold as defined in FAR 2.101 on the date of subcontract award.

(End of clause)

52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (DEVIATION 2020-05)
(April 10, 2020)

(a) *Definitions*. As used in this clause—

"Covered article" means any hardware, software, or service that–

(1) Is developed or provided by a covered entity;

(2) Includes any hardware, software, or service developed or provided in whole or in part by a covered entity; or

(3) Contains components using any hardware or software developed in whole or in part by a covered entity.

"Covered entity" means–

(1) Kaspersky Lab;

(2) Any successor entity to Kaspersky Lab;

(3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or

(4) Any entity of which Kaspersky Lab has a majority ownership.

(b) *Prohibition*. Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits Government use of any covered article. The Contractor is prohibited from—

(1) Providing any covered article that the Government will use on or after October 1, 2018; and

(2) Using any covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the contract.

(c) *Reporting requirement*.

(1) In the event the Contractor identifies a covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or any other source, the Contractor shall report, in writing via email, to the Contracting Officer, Contracting Officer's Representative, and the Enterprise Security Operations Center (SOC) at (b)(7)(E), with required information contained in the body of the email. In the case of the Department of Defense, the Contractor shall report to the website at (b)(7)(E) For indefinite delivery contracts, the Contractor shall report to the Enterprise SOC, Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) and Contracting Officer's Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at (b)(7)(E)

(2) The Contractor shall report the following information pursuant to paragraph (c)(1) of this clause:

(i) Within 1 business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; brand; model number (Original Equipment Manufacturer (OEM) number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the report pursuant to paragraph (c)(1) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of a covered article, any reasons that led to the use or submission of the covered article, and any additional efforts that will be incorporated to prevent future use or submission of covered articles.

(d) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts, including subcontracts for the acquisition of commercial items.

(End of clause)

FAR 52.204-25 Prohibition On Contracting For Certain Telecommunications And Video Surveillance Services Or Equipment (Deviation 20-05) (Aug 2020)

(a) *Definitions.* As used in this clause—

"Backhaul" means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

"Covered foreign country" means The People's Republic of China.

"Covered telecommunications equipment or services" means–

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

"Critical technology" means–

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);
(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

"Interconnection arrangements" means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

"Reasonable inquiry" means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

"Roaming" means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

"Substantial or essential component" means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) Prohibition.

(c) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115–232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115–232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an

entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) *Exceptions.* This clause does not prohibit contractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement.

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause in writing via email to the Contracting Officer, Contracting Officer's Representative, and the Enterprise Security Operations Center (SOC) at [redacted] with required information in the body of the email. In the case of the Department of Defense, the Contractor shall report to the website at [redacted] For indefinite delivery contracts, the Contractor shall report to the Enterprise SOC, Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) and Contracting Officer's Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at [redacted]

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or

submission of covered telecommunications equipment or services.

(e) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (e), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

FAR 52.217-8 Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within one day prior to contract expiration.

(End of clause)

FAR 52.217-9 Option to Extend the Term of the Contract (Mar 2000)

(a)The Government may extend the term of this contract by written notice to the Contractor within *one day prior to contract expiration*; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least *30 calendar days* before the contract expires. The preliminary notice does not commit the Government to an extension.

(b)If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c)The total duration of this contract, including the exercise of any options under this clause, shall not exceed *five years, six months*.

(End of clause)

FAR Deviation Clauses incorporated by Full Text:

FAR 52.204-23 PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES (DEVIATION 2020-05) (APRIL 10, 2020)

(a) *Definitions*. As used in this clause—

"Covered article" means any hardware, software, or service that–

(1) Is developed or provided by a covered entity;

(2) Includes any hardware, software, or service developed or provided in whole or in part by a covered entity; or

(3) Contains components using any hardware or software developed in whole or in part by a covered entity.

"Covered entity" means–

(1) Kaspersky Lab;
(2) Any successor entity to Kaspersky Lab;
(3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or
(4) Any entity of which Kaspersky Lab has a majority ownership.

(b) *Prohibition*. Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits Government use of any covered article. The Contractor is prohibited from—

(1) Providing any covered article that the Government will use on or after October 1, 2018; and
(2) Using any covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the contract.

(c) *Reporting requirement*.

(1) In the event the Contractor identifies a covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or any other source, the Contractor shall report, in writing via email, to the Contracting Officer, Contracting Officer's Representative, and the Enterprise Security Operations Center (SOC) at (b)(7)(E) with required information contained in the body of the email. In the case of the Department of Defense, the Contractor shall report to the website at (b)(7)(E) For indefinite delivery contracts, the Contractor shall report to the Enterprise SOC, Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) and Contracting Officer's Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at (b)(7)(E)

(2) The Contractor shall report the following information pursuant to paragraph (c)(1) of this clause:

(i) Within 1 business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; brand; model number (Original Equipment Manufacturer (OEM) number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the report pursuant to paragraph (c)(1) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of a covered article, any reasons that led to the use or submission of the covered article, and any additional efforts that will be incorporated to prevent future use or submission of covered articles.

(d) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts, including subcontracts for the acquisition of commercial items.

(End of clause)

FAR 52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (DEVIATION 20-05) (AUG 2020)

(a) *Definitions.* As used in this clause—

"Backhaul" means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core

telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

"Covered foreign country" means The People's Republic of China.

"Covered telecommunications equipment or services" means–

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

"Critical technology" means–

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);
(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

"Interconnection arrangements" means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

"Reasonable inquiry" means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

"Roaming" means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

"Substantial or essential component" means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) *Prohibition.*

(1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115–232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115–232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) *Exceptions.* This clause does not prohibit contractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) *Reporting requirement.*

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause in writing via email to the Contracting Officer, Contracting Officer's Representative, and the Enterprise Security Operations Center (SOC) at (b)(7)(E), with required information in the body of the email. In the case of the Department of Defense, the Contractor shall report to the website at (b)(7)(E). For indefinite delivery contracts, the Contractor shall report to the Enterprise SOC, Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) and Contracting Officer's Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at (b)(7)(E).

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (e), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

FAR 52.232-40 Providing Accelerated Payments to Small Business Subcontractors. (DEC 2013) (DEVIATION APR 2020)

(a)(1) In accordance with 31 U.S.C. 3903 and 10 U.S.C. 2307, upon receipt of accelerated payments from the Government, the Contractor shall make accelerated payments to its small business subcontractors under this contract in accordance with the accelerated payment date established, to the maximum extent

practicable and prior to when such payment is otherwise required under the applicable contract or subcontract, with a goal of 15 days after receipt of a proper invoice and all other required documentation from the small business subcontractor if a specific payment date is not established by contract.
(2) The Contractor agrees to make such payments to its small business subcontractors without any further consideration from or fees charged to the subcontractor.
(b) The acceleration of payments under this clause does not provide any new rights under the Prompt Payment Act.
(c) Include the substance of this clause, including this paragraph (c), in all subcontracts with small business concerns, including subcontracts with small business concerns for the acquisition of commercial items.

(End of clause)

HSAR Clauses incorporated by Reference:

[*Contracting Officer check as appropriate.*]

X 3052.203-70, Instructions for Contractor Disclosure of Violations (Sep 2012)

X 3052.205-70, Advertisements, Publicizing Awards, and Releases (Sep 2012)

_3052.209-71, Reserve Officer Training Corps and Military Recruiting on Campus (Dec 2003)

X 3052.219-70 Small Business Subcontracting Plan Reporting (Jun 2006)

X 3052.219-71 DHS Mentor Protégé Program (Jun 2006)

X 3052.219-72 Evaluation of Prime Contractor Participation in DHS Mentor Protégé Program (Jun 2006)

X 3052.242-72 Contracting Officer's Technical Representative (Dec 2003)

HSAR Clauses in full text

HSAR 3052.204-71 Contractor Employee Access (Sep 2012)

(a) *Sensitive Information,* as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Pub. L. 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially

communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, part 1520, as amended, Policies and Procedures of Safeguarding and Control of SSI, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as For Official Use Only, which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated sensitive or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) Information Technology Resources include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(End of clause)

***Alternate II* (JUN 2006)** When the Department has determined contract employee access to sensitive information or Government facilities must be limited to U.S. citizens and lawful permanent residents, but the contract will not require access to IT resources, add the following paragraphs:

(g) Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident Card (USCIS I-551). Any exceptions must be approved by the Department's Chief Security Officer or designee.

(h) Contractors shall identify in their proposals, the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the Contracting Officer.

(End of clause)

Special Clause Safeguarding of Sensitive Information (Mar 2015)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Definitions*. As used in this clause—

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or

homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107- 296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

"Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) *Authorities.* The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
(2) DHS Sensitive Systems Policy Directive 4300A
(3) DHS 4300A Sensitive Systems Handbook and Attachments
(4) DHS Security Authorization Process Guide
(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
(7) DHS Information Security Performance Plan (current fiscal year)
(8) DHS Privacy Incident Handling Guidance
(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html
(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

(d) *Handling of Sensitive Information.* Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL

USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA),* as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) *Authority to Operate*. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 9.1, July 24, 2012), or any successor publication, and the *Security Authorization Process Guide* including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment

Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods:
(1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls;

or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) *Security Review.* The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Continuous Monitoring.* All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this
contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall

comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) Sensitive Information Incident Reporting Requirements.

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime contractor location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
(v) Contracting Officer POC (address, telephone, email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms or systems involved;

(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

(g) Sensitive Information Incident Response Requirements.

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(i) Inspections,
(ii) Investigations,
(iii) Forensic reviews, and
(iv) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(h) *Additional PII and/or SPII Notification Requirements.*

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the DHS Privacy Incident Handling Guidance. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;
(ii) A description of the types of PII and SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;
(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(i) *Credit Monitoring Requirements*. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and

(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*.

(End of Special Clause)

Special Clause Information Technology Security and Privacy Training (Mar 2015)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Security Training Requirements*.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting

sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

(c) *Privacy Training Requirements.* All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting Personal Information* before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors.

Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e- mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(End of clause)

Performance Work Statement (PWS)
Department of Homeland Security (DHS),
Immigration and Customs Enforcement (ICE)
Law Enforcement Investigative Database Subscription
December 3, 2020

1. BACKGROUND

The intent of this Performance Work Statement (PWS) is to procure a web-based law enforcement investigative database subscription service to assist Immigration, Customs and Enforcement (ICE) mission of conducting criminal investigations that protect the United States against terrorists and criminal organizations that threaten our safety and national security; to combat transnational criminal enterprises that see to exploit America's legitimate trade, travel and financial systems. ICE investigative agents require a robust analytical research tool for its in-depth exploration of persons of interest and vehicles.

The purpose of this contract is to provide ICE agents an investigative database system to further strategize arrests to minimize and, in some cases, avoid impact of potential injury. ICE requirement of a web-based law enforcement investigative database platform is to include, integration access to public records and commercial data with uninterrupted service, integrate investigative capabilities with the license plate recognition capabilities to be utilized by multiple ICE Directorates to include but not limited to Homeland Security Investigative (HSI), Enforcement and Removal Operations (ERO) and Office of Professional Responsibility (OPR). Use of this database subscription services furthers the criminal law enforcement mission.

1.1 **DHS/ICE**

ICE is the largest investigative agency in the Department of Homeland Security (DHS) and was formally established on March 1, 2003. ICE's primary mission is to protect national security, public safety, and the integrity of the US borders through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration.

ICE investigates a range of domestic and international activities including:

- Human smuggling and trafficking;
- Narcotics, cultural property, weapons and other contraband smuggling;
- Export enforcement, e.g., illegal arms and dual-use equipment;
- Financial crimes;
- Commercial fraud;
- Intellectual property rights violations;
- Cyber-crimes;
- Immigration fraud; and,
- Human rights violations.

The law enforcement investigative database system currently supports over 11,000 users across multiple program areas with analytical data and concrete information to search high risk and

politically exposed criminal activity worldwide. The database subscription service plays a crucial role in ICEs overall investigative mission success. Moreover, the agency can achieve cost savings to the government when reducing the work hours required for physical surveillance.

2.0 SCOPE/OBJECTIVES

The Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement (ICE) houses a large dataset of detailed data that is available to an assortment of approved law enforcement users. ICE criminal law enforcement mission; to enhance investigations to support all mission activities mentioned above in over 50 countries and 67 locations globally; to provide a platform where the continuity of public records and commercial data is available on an uninterrupted basis and to identify criminal suspects, businesses and assets of targets of investigations for potential arrest, seizure and forfeiture will require the usage of a robust investigative database subscription service.

The scope of this requirement is to subscribe to and use the contractor's proprietary data, content and analytical data to optimize ICE operational support functions to enable mission success. This includes supporting all aspects of ICE screening and vetting, lead development, and criminal analysis activities. It also includes, but is not limited to, conducting data extractions to identify unusual trends, data anomalies, and control breakdowns, identifying possible trends, patterns, and links to automate methods for detecting, monitoring, analyzing, summarizing and graphically representing patterns of relationships between entities, identifying potentially criminal and fraudulent behavior before crime and fraud can materialize, and detecting and reporting elements of crimes involving the exploitation or attempts to exploit the immigration and customs laws of the United States.

ICE requires web-based law enforcement investigative databases platform to provide constant (24 hour, seven days per week, 365 days a year) accessibility to a database for ICE law enforcement personnel across the United States in the execution of their official law enforcement duties.

The task areas listed constitute the technical scope of this PWS:

- Task Area 1: Database Functionality Requirements (CLIN 0001)
- Task Area 1A: Training and User Management Support (CLIN 0002)
- Task Area 2: License Plate Reader (LPR) (CLIN 0003)
- Task Area 2A: License Plate Reader Training and User Management Support (CLIN 0004)

Contractor shall provide database access to 11,000 users.

3.0 TASK REQUIREMENTS

The ICE law enforcement investigative database platform shall contain a web-based, centralized database for client management and reporting. Generally, all users shall provide direct input into the database and output requests (reports) shall be generated directly from the database system.

The ICE participating programs shall provide input (i.e., client level data) and the contractor shall provide the database systems administrative and support for report generation. The

investigative platform requires the best-supported investigative data and data-analytic management available in the marketplace; to allow readily available access to billions of public records and additional investigative content in an intuitive working environment.

The tasks required under this Performance Work Statement (PWS) require a community-wide data-analytic collection and management system that includes the following:

3.1 TASK AREA 1: DATABASE FUNCTIONAL REQUIREMENTS

- The government's requirement is that the database uses a matching algorithm to return search records that can identify and eliminate duplicated results. The database shall use Entity Resolution applied across results from all sources as they are returned. This maximizes the value of searching multiple sources and saves time by automating the process of record comparison.
- The government's requirement is that the database must be able to interface with FALCON/Raven Palantir systems. The database program shall offer a system-to-system (S2S) connection that merges the database program's public and proprietary data with Palantir analytical information to narrow in and locate persons and assets of interest. (S2S application-programming interface (API) will replace Palantir connection)
- The government's requirement is that the database must compare the input search criteria and score them against all records in their data sources. The database must use a Relevant Scoring application that allows them to return the most relevant and most current records at the top of the results list.
- The government's requirement is that the database program must have the ability to construct link charts. The database shall use Link-Chart Visualization and Mapping, which allows investigators to save selected results and report data indefinitely and provides the capability to generate link charts and map views of the data.
- The government's requirement is that the database program must allow for multiple searches using unique criteria. Investigators must be allowed to enter specific search criteria once, the system then returns all relevant data, regardless of the source. The program must support search federation against both open-source and internal data repositories and include features like entity resolution, search filtering and charting and mapping across all supported sources.
- The government's requirement is that the database program must allow for Batch Requests where multiple social security numbers (SSN) and or phone numbers may be queried at one time. This capability is both time- and cost-saving for Worksite and Identity Benefit Fraud investigations where multiple SSN's are queried at one time vs. one at a time.
- The government's requirement is that the database must allow for mobile "on the go" access. The law enforcement investigative research tool shall provide full access to core search and report capability from mobile, wireless devices, including HTML5-supported smartphones.
- Available functionality includes person, vehicle, watercraft and phone searches and the National Comprehensive Report. Reports shall be saved automatically in a

results tab for future viewing.

- The government's requirement is that the database shall have the ability to conform to the investigator's needs, so reports generated can be customized to an investigator or analyst case load. Users shall create report templates by setting report preferences, identifying which sections to include, and setting the sequence in which sections are displayed. For example, customers wanting to see only the asset-related information for an individual could create an "Asset Profile" report with the sections they want included, in the order that they want. The law enforcement online research tool shall also offer a workspace feature which allows users to save selected results and report data indefinitely and provides the ability to generate link-chart and map views of the data. Visualizing information on multiple subjects in a link-chart view makes it easier for investigators to discern possible connections or associations between subjects/entities.
- The government's requirement is that the information provided by the law enforcement online research tool should enable ICE to effectively and quickly identify assets currently owned or previously owned/operated by suspect individuals and/or organizations under investigation. The research tool should allow for the flexibility of locating suspects' assets through a multitude of search options. It should also offer the ability to create custom searches so investigators can retrieve information more specific to the time of criminal activity and/or by target name.
- The government's requirement is that the information provided by the law enforcement online research tool should enable ICE OPR to effectively identify searching of a record/document and generate a corresponding audit record. The system shall allow OPR to search sign-on data for the user profile based on a beginning and ending date and time.

- The government's requirement is the system will have the capacity to:
    - Generate program, agency, community, and, if applicable, collaborative level reports.
    - Produce standard, built-in reports and forms to be queried by Area of Responsibility (AOR), to include user reports, agency reports, component, location and sublocation reports and other reports as required.
    - Perform integrated ad hoc reporting that maintains user level security restrictions while allowing for user flexibility in choosing tables and fields as well as filtering and conditional report aspects.
    - Import and export data through XML and CSV formats, imports and exports and ability to securely strip data of identifiers and manage data transmission.
- The government's requirement is that System Security will include Integrated technical safeguards to ensure a high level of privacy and security, including:
    - Back end server(s), including data encryption and transmission
    - Administrator controlled username and password access
    - Automatic timeout/log-off
    - Administrator controlled user level read, write, edit and delete capabilities

- Administrator controlled user level module and sub-module access
- Automated audit trail
- Information Security Industry Standard encryption and SSL certifications (256-Bit AES encryption)

All technical safeguards required to protect Personally Identifiable Information (PII) All security safeguards required for compliance.

3.2 TASK AREA 2: LICENSE PLATE READER (LPR) REQUIREMENTS

- The LPR data service shall contain LPR records from a variety of sources across the United States, such as publicly accessible toll roads or parking lot cameras, vehicles repossession companies and law enforcement agencies.
- The LPR data service shall include substantial unique LPR detection records.
- The LPR data service shall compile LPR from at least 25 states and 24 of the top 30 most populous metropolitan statistical areas to the extend authorized by law in those locations.
    - A metropolitan statistical area is defined as: a geographical region with a relatively high population density at its core and close economic ties throughout the area as defined by the Office of Management and Budget (OMB) and used by the Census Bureau and other federal government agencies for statistical purposes.
- The LPR data service provider shall demonstrate the number of new unique records that were added to the commercially available LPR database each month for the last consecutive twelve (12) months.
- The LPR data service shall make available at least 30 million new unique LPR data records each month.

3.2.1 QUERY CAPABILITIES

- The contract shall ensure that before a user is able to perform a query from the database or mobile application; the tool must display upon logon a splash screen that describes the agency's permissible uses of the database application, the data and all user's affirmative consent to the rules of behavior prior to initial entry of the investigative tool.
- The contractor shall ensure the splash screen shall appear at each logon event.
- The contractor shall ensure the text on the splash screen shall also be available to the users via a hyperlink within the main system interface (to include mobile app interface)
- The contractor shall provide the language for the splash screen content.
- The contractor shall ensure that queries of the LPR data service can be based on a complete or partial license plate number queried by the user only and the data returned in response must be limited to matches of that license plate number only within the specified period of time.
- The contractor shall create separate log-on environments for ICE personnel authorized to perform advanced queries. One environment will appear for users who must enter a license plate number (full or partial) or other non-geographical

coordinate based restrictions to query the database, and the other environment will appear for users authorized to search by geographic area.

- The query interface shall include a drop-down field for users to select a reason code for the query from a pre-populated list. The specific reason codes shall be provided by ICE. This field is mandatory for conducting a query.
- The contractor shall ensure geographic queries also include a common plate search feature. A common plate search allows investigators to analyze multiple locations to see if any license plate(s) appeared in the selected locations.
- The query interface will require the user to identify whether the user is entering data for either him or herself or for another individual. If the user is entering data for another individual, the query interface will require the user to enter the name of the other individual.
- The query interface must include a free-text field of at least 255 alphanumeric characters for user notes. This will allow for additional information that will assist ICE in referencing the specific case for which the query was performed. Completing this field shall be mandatory for conducting a query.
- The system will have the capability to limit the query by time frame to allow users to comply with agency policy. Depending on the type of investigation being conducted, agency policy will allow the user to query the historical LPR detection records for only a certain period of time (e.g., going back 5 years from the date of query for any immigration investigation).
    - The query interface will have a field for the user to select or input the appropriate timeframe for the query.
    - The system will display results only for LPR detection records within that timeframe (e.g., only for the last 5 years).
    - The system shall not run a query that lacks a time frame entered by the user.
        - The contractor shall guarantee the results of queries meet a high degree of accuracy in datasets, with a margin of error not more than 2%.
        - To ensure accuracy of information, the response to a query must include at least two photos on all hits.
        - Photos must be of sufficient quality to allow the user to visually confirm the license plate and vehicle make/model in the photo are the same as what is represented in the contractor system.
        - Query results must seamlessly integrate with web-based interactive maps. The printable report should show two different map views, nearest address, nearest intersection and coordinates.
        - The contractor shall provide a notification mechanism in the event ICE users identify photographs that do not match the data in their system (license plate numbers or make/model mismatches). The contractor shall address all erroneous data. The contractor shall notify ICE and the ICE user of any inputted erroneous data and keep ICE and ICE users informed of corrections to erroneous data.

- The contractor will not use any information provided by the agency (query data) for its own purposes or share the information with other customers, business partners, or any other entity.

- The contractor will not use ICE's queries (the license plate numbers input into the system) for its commercial purposes. The contractor will only use the queries submitted by ICE to maintain an audit log.
- The contractor will ensure ICE user queries are conducted anonymously to ensure other individuals or entities that use the LPR service (whether a law enforcement agency, commercial entity, or otherwise) are not able to identify that ICE is investigating a license plate.

3.2.2 ALERT LIST CAPABILITIES

- The LPR data service shall provide an "Alert List" feature that will save license plate numbers to query them against new records loaded into the contractor's LPR database on an on-going basis. Any matches will result in a near real-time notification to the user who queried the license plate number.
- The LPR data service Alert List will provide capabilities to share Alert List notifications between ICE users involved in the investigation.
- The Alert List feature will: 1) Automatically match new incoming detection records to user-uploaded or -entered Alert Lists containing the license plate numbers of interest in the investigation; 2) Send an email notification to the user originating such Alert List records and to any ICE user that has been shared the Alert List indicating there is a license plate match to new records in the system; and 3) Provide within the LPR system for download a PDF case file report for the match (with maps, vehicle images, and all pertinent detection & Alert List record information) for each email alert notification. The notification must be able to be limited to the user or a user group of ICE law enforcement officers involved in the specific investigation. The notification will comply with all applicable laws, including the Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725.
- The LPR data service will allow specifically designated users to batch upload a maximum of 2,500 license plate records into the "Alert List". The batch upload will be in the form of a single comma separated variable (CSV) file with data fields to include, but not limited to the following: Plate number; State of Registration; Vehicle Year, Make, Model & Color; reason code and an open text field, of at least 255 alphanumeric characters for a user note to assist in referencing the specific purpose / investigation / operation for which the query was performed.
- The contractor will provide the ability to establish Alert List submissions, flag license plates for deconfliction, and perform searches, all conducted anonymously, to ensure other individuals or entities that use the LPR service (whether a law enforcement agency, commercial entity, or otherwise) are not able to identify that ICE is investigating a license plate.
- License plate pictures taken with the automated Optical Character Recognition (OCR) plate number translation shall be submitted to the LPR data service system for matching with license plates on any current ICE Alert List. Any positive matches shall return to the iOS application (identified below) alerting authorized users of a positive match. These pictures will be uploaded into the data service query by an authorized ICE user along with any mandatory information needed for a normal query.

- Each license plate number on an Alert List will be valid for one year unless the user removes it before expiration. The system will prompt users prior to expiration and allow the user to keep the particular Alert List or license plate number active or be given the option to delete the license plate from the Alert List. If the user does not renew, the system shall remove the license plate number from the Alert List.
- All Alert List activity shall be audited to capture username, date and time, reason code, and user note associated with the query, as well as license plate number entry, deletion, renewal, and expiration from the alert list.
- Have quick access and recall of any queries and Alert Lists associated with the user or designated user group. The contractor application will delete any saved data on the mobile device after 60 days, if not already deleted manually by the user.
- The contractor shall not retain any data entered onto an Alert List except as part of the audit trail once the entry has expired per the process described above, or once the user has deleted the entry from the Alert List.

3.2.3 MOBILE DEVICE CAPABILITIES

- The LPR data service shall feature an iOS-compatible mobile application that allows authorized ICE users to:
- Query the LPR data service by entering the license plate number (complete/partial), state of registration, reason code, and the ability to add returned positive matches into the Alert List.
- The contractor shall ensure the mobile application allows the user to scan vehicle plates (full and/or partial), using their mobile device camera, which are automatically uploaded into the contractor's database and queried against various hotlists in the existing IOS/Android compatible applications.
- The contractor shall ensure the mobile application has a mobile alert feature. Scanned plates are sent as detections to the contractor's law enforcement archival and reporting network which could trigger alert notifications. The mobile alert shall enable an alert banner display in near real time if a scanned plate is a shared hot list match.
- Queries can be performed by inputting geographic area (for authorized users).
- The mobile application will conform all other performance, privacy, and functional requirements identified in the PWS. The contractor shall coordinate with ICE to make sure that the mobile application undergoes the required privacy assessment prior to use.

3.2.4 AUDIT AND REPORTING CAPABILITIES

- The contractor shall generate an immutable audit log in electronic form that chronicles the following data:
    - Identity of the user initiating the query or the person on whose behalf the query is initiated, if different;
    - Exact query entered, to include license plate number, date limitations, geographic limitations (if applicable), reason code, and any other data selected or input by the user;

- Date and time of query; and
- Results of the query.

- All Alert List activity shall be audited to capture username, date and time, reason code, and user note associated with the query, as well as license plate number entry, deletion, renewal, and expiration from the alert list.

- The contractor shall provide to ICE user audit reports upon request. Audit reports shall contain the audit log information of a given user(s) for the specified period of time. The contractor shall provide the audit log in electronic form via secure transmission to ICE promptly upon request. The format of the audit log shall allow for ICE to retrieve user activity by username (or ID), query entered (e.g., particular license plate) and date/time. The exact technical requirements and format for the audit log will be negotiated after contract award.

- The contractor shall promptly cooperate with an ICE request to retrieve and provide a copy of the actual records retrieved from the LPR data service in response to a particular query, or any other data relevant to user activity on the contractor system, for purposes of the agency's internal investigations and oversight.

- The contractor shall not use audit trail data for any purpose other than those specified and authorized in this contract.

- The contractor is to provide monthly and upon request, statistics based on positive hits against the number of requested searches and hit list.

- The audit logs specified in this statement of work are records under the Federal Records Act. The contractor shall maintain these records on behalf of ICE throughout the life of the contract, but for no more than seven (7) years. The contractor is not authorized to share these records, or the Alert List data, with any outside entities including other law enforcement agencies. At the end of the contract, the contractor shall extract, transfer, and load these records (including any still-active Alert List data, if requested by ICE) to another storage medium or location specified by ICE. This transfer of records shall occur no later than thirty (30) days after the contract ends. After successful transfer of these records, the contractor shall ensure all copies of the records (including any still-active Alert List data) are securely deleted from all networks and storage media under its control or under the control of any of its agents or subcontractors.

- The contractor shall meet the following Key Performance Parameters (KPPs):

Metric	Unit of Measure	Minimum
LPR Data Service	Uptime – Unit of measure 100%	>99.0
	Operating Schedule	24/7/365
	Scheduled downtime	</= 4 hours per month
	Meantime between failure (MTBF)	4,000 operating hours

Overall Support Service	Support availability	24/7/365
Results of LPR Query	Results of a single LPR query	</= 5 seconds after submission

3.3 TASK AREAS 1A and 2A: TRAINING AND USER MANAGEMENT SUPPORT.

The object of this task is to provide training to ICE personnel through on-site, remote, and/or on-demand training on the Law Enforcement Investigative database tool. Training and user management support is implemented to ensure proper guidance and navigation of the database tool is accessible to all assigned users.

- The contract shall provide written instruction manuals and guidance to facilitate use of the database investigative tool and the LPR system.

- The contract shall ensure the user has the ability to compare new user requests with lists of personnel authorized by ICE to utilize the database and LPR tool.

- The contractor shall ensure that all users has automatic verification of accounts with the ability to audit by using the user's Originating Agency Identifier (ORI) to be matched against a current real-time list of active ORI numbers provided directly or indirectly by the National Law Enforcement Telecommunications System (NLETS).

- The contractor shall have the ability to add new users or delete existing users within 24 business hours of ICEs request.

- The contract shall provide initial training or subsequent training to orient persons to the use of the database investigative and LPR tool; to include the "Help Desk" support related to the use, access and maintenance of the tool.

- The contractor shall provide customized training on-site, telephone and web-based training to include webinars and "on demand" classes and electronic quick reference guides for users. On-site training shall be limited to the Washington, DC location with a maximum of 2 training visits per year.

- The contract shall provide system training and escalation procedures as it pertains to agency administrators and shall include procedures for password resets to the database tool.

- The contractor shall provide unlimited technical support for all users.

- The contractor shall perform periodic or as needed updates (maintenance, refresh, etc.) to the overall database tool, web-based interface and mobile application. The contractor shall also ensure to employ appropriate technical, administrative and physical security controls are in place to protect the integrity, availability and confidentiality of the data that resides on all of its systems.

4.0 OTHER APPLICABLE REQUIREMENTS

4.1 PERIOD OF PERFORMANCE

The Period of Performance will consist of a base year with four (4) one-year options.

4.2 PLACE OF PERFORMANCE

The primary place of performance will be the Contractor's facilities with frequent visits to the, Immigration and Customs Enforcement (ICE) headquarters facilities in the Washington Metro Area.

4.3 TRAVEL

Contractor travel is not required for this requirement. Local meetings or activities planned outside of the defined place of performance are permitted, but all expenses incurred are the responsibility of the contractor.

4.4 POST AWARD CONFERENCE

The Contractor shall attend Post Award Conference with the Contracting Officer and the COR no later than 5 business days after the date of award. The purpose of the Post Award Conference, which will be chaired by the Contracting Officer, is to discuss technical and contracting objectives of this contract. The Post Award Conference will be held either virtually (e.g., MS Teams, Zoom, Adobe Connect, etc.) and/or at the Government's facility, location to be determined via teleconference.

4.5 INVOICES

A standard invoice template shall be provided by the contractor and confirmed by the COR for use on this contract. Invoices shall be verified by the Government COR and submitted on a monthly basis.

4.6 CONTRACTOR QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

The Contractor shall establish and maintain a Quality Assurance Surveillance Plan (QASP) to ensure the requirements of this contract are provided as specified. The Contractor shall provide a QASP describing the inspection system that they intend to use for the requested services listed. The contractor shall implement procedures to identify, prevent and ensure non-recurrence of defective services. The Contractor's draft QASP shall be required as part of their quote submittal. The CO will notify the Contractor of acceptance or the necessity for QASP modification of the plan no later than 10 business days after award. The Contractor shall provide a final QASP to the COR no later than 20 business days after award. The QASP shall be updated as changes occur and shall be submitted to the COR for review and subsequent CO acceptance by the government. The Performance Requirements Summary (PRS) and Performance Standards Matrix (PSM) is outlined in the Quality Assurance Surveillance Plan (QASP) Appendix A.

5.0 DELIVERABLES

The contractor shall provide the following deliverables in the format and frequency listed.

Deliverables Name	PWS Paragraph	Frequency
Kick-off Meeting/Post Award Conference	4.4	A kick-off meeting with the government will be conducted within 5 days of award. Meeting minutes due from Contractor to COR & CO within 2 business days of the meeting.
Audit report, ad hoc reports, user manuals, etc.	3.2.4 3.3	Reports are due upon request of the COR and/or as required. To include any subsequent updates.
Audit Logs, transfer of records	3.2.4	Provide email confirmation 30 days after contract ends.
Data Rights any work first produced such as user administrative and operations manuals and anything else first produced under this PWS if applicable.		One month prior to the end of the period of performance (POP).
QASP/Progress Reports	4.7	Draft due to the government proposal. Final QASP due to the COR and CO 20 days after award. Subsequent reports due quarterly and/or as requested.
Invoices	4.5	Invoice should be submitted on a monthly basis to the COR and designated Finance Center for all services performed and no more than 30 days in the arrears of the last day of the POP.

5.1 GENERAL REPORT REQUIREMENTS

The Contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with ICE workstations (Windows XP and Microsoft Office Applications).

5.2 ACCEPTANCE CRITERIA

ICE will accept or reject deliverables within fifteen (15) business days after delivery. If rejected, the Contractor shall make corrections as specified and resubmit the deliverable for review and approval within five (5) business days provided however that contractor is not dependent upon a third party for performance. If the government does not reply within the specific timeframe than the deliverable shall be determined acceptable.

6.0 SECTION 508 COMPLIANCE

Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) as amended by P.L. 105-220 under Title IV (Rehabilitation Act Amendments of 1998) all Electronic and Information Technology (EIT) developed, procured, maintained and/or used under this contract shall be in compliance with the "Electronic and Information Technology Accessibility Standards" set forth by the Architectural and Transportation Barriers Compliance Board (also referred to as the "Access Board") in 36 CFR Part 1194. The complete text of Section 508 Standards can be accessed at http://www.access-board.gov/ or at http://www.section508.gov.

7.0 PRIVACY REQUIREMENTS

Limiting Access to Privacy Act and Other Sensitive Information
In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984), and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires contractor personnel to have access to information protected by the Privacy Act of 1974, the contractor is advised that the relevant DHS system of records notices (SORNs) applicable to this Privacy Act information may be found at https://www.dhs.gov/system-records-notices-sorns. Applicable SORNS of other agencies may be accessed through the agencies' websites or by searching GovInfo, available at https://www.govinfo.gov that replaced the FDsys website in December 2018. SORNs may be updated at any time.

Prohibition on Performing Work Outside a Government Facility/Network/Equipment
The Contractor shall perform all tasks on authorized Government networks, using Government-furnished IT and other equipment and/or Workplace as a Service (WaaS) if WaaS is authorized by the statement of work. Government information shall remain within the confines of authorized Government networks at all times. Except where telework is specifically authorized within this contract, the Contractor shall perform all tasks described in this document at authorized Government facilities; the Contractor is prohibited from performing these tasks at or removing Government-furnished information to any other facility; and Government information shall remain within the confines of authorized Government facilities at all times. Contractors may only access classified materials on government furnished equipment in authorized government owned facilities regardless of telework authorizations.

Prior Approval Required to Hire Subcontractors
The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (Subcontractor) in support of this contract requiring the disclosure of

information, documentary material and/or records generated under or relating to this contract. The Contractor (and any Subcontractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

Separation Checklist for Contractor Employees
Contractor shall complete a separation checklist before any employee or Subcontractor employee terminates working on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposal of sensitive personally identifiable information (PII), in paper or electronic form, in the custody of the employee or Subcontractor employee including the sanitization of data on any computer systems or media as appropriate; and (3) termination of any technological access to the Contractor's facilities or systems that would permit the terminated employee's access to sensitive PII.
In the event of adverse job actions resulting in the dismissal of an employee or Subcontractor employee, the Contractor shall notify the Contracting Officer's Representative (COR) within 24 hours. For normal separations, the Contractor shall submit the checklist on the last day of employment or work on the contract.

As requested, contractors shall assist the ICE Point of Contact (ICE/POC), Contracting Officer, or COR with completing ICE Form 50-005/Contractor Employee Separation Clearance Checklist by returning all Government-furnished property including but not limited to computer equipment, media, credentials and passports, smart cards, mobile devices, PIV cards, calling cards, and keys and terminating access to all user accounts and systems.

Contractor's Commercial License Agreement and Government Electronic Information Rights
Except as stated in the Performance Work Statement and, where applicable, the Contractor's Commercial License Agreement, the Government Agency owns the rights to all electronic information (electronic data, electronic information systems or electronic databases) and all supporting documentation and associated metadata created as part of this contract. All deliverables (including all data and records) under the contract are the property of the U.S. Government and are considered federal records, for which the Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

Privacy Lead Requirements
If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy documentation, the Contractor shall assign or procure a Privacy Lead, to be listed under the SOW or PWS's required Contractor Personnel section. The Privacy Lead shall be responsible for providing adequate support to DHS to ensure DHS can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance. The Privacy Lead shall work with personnel from the program office, the ICE Privacy Unit, the Office of the Chief Information Officer, and the Records and Data Management Unit to ensure that the privacy documentation is kept on schedule, that the answers to questions in the PIA are thorough and complete, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.

The Privacy Lead:

- Must have excellent writing skills, the ability to explain technology clearly for a non-technical audience, and the ability to synthesize information from a variety of sources.
- Must have excellent verbal communication and organizational skills.
- Must have experience writing PIAs. Ideally the candidate would have experience writing PIAs for DHS.
- Must be knowledgeable about the Privacy Act of 1974 and the E-Government Act of 2002.
- Must be able to work well with others.

If a Privacy Lead is already in place with the program office and the contract involves IT system builds or substantial changes that may require privacy documentation, the requirement for a separate Private Lead specifically assigned under this contract may be waived provided the Contractor agrees to have the existing Privacy Lead coordinate with and support the ICE Privacy POC to ensure privacy concerns are proactively reviewed and so ICE can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance if required. The Contractor shall work with personnel from the program office, the ICE Office of Information Governance and Privacy, and the Office of the Chief Information Officer to ensure that the privacy documentation is kept on schedule, that the answers to questions in any privacy documents are thorough and complete, that all records management requirements are met, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.

Quality Assurance Surveillance Plan (QASP)
Law Enforcement Investigative Database Service

NOTE: The Government reserves the right to revise or change the QASP as determined by the Government to ensure quality service and deliverables over the course of the contract.

1. PURPOSE

This Quality Assurance Surveillance Plan (QASP) provides a systematic method to evaluate performance for the stated contract. This QASP explains the following:

- What will be monitored
- How monitoring will take place
- Who will conduct the monitoring
- How monitoring efforts and results will be documented

This QASP does not detail how the Contractor accomplishes the work. Rather, the QASP is created with the premise that the Contractor is responsible for management and quality control actions to meet the terms of the contract. It is the Government's responsibility to be objective, fair, and consistent in evaluating performance. In addition, the QASP should recognize that unforeseen and uncontrollable situations may occur.

This QASP is a "living document" and the Government may review and revise it on a regular basis. However, the Government shall coordinate changes with the Contractor. Updates shall ensure that the QASP remains a valid, useful, and enforceable document. Copies of the original QASP and revisions shall be provided to the Contractor and Government officials implementing surveillance activities.

2. GOVERNMENT ROLES AND RESPONSIBILITIES

The following personnel shall oversee and coordinate surveillance activities.

a. Contracting Officer (CO) - The CO shall ensure performance of all necessary actions for effective contracting, ensure compliance with the contract terms, and shall safeguard the interests of the United States in the contractual relationship. The CO shall also ensure that the Contractor receives impartial, fair, and equitable treatment under this contract. The CO is ultimately responsible for the final determination of the adequacy of the Contractor's performance.

b. Contracting Officer's Representative (COR) - The COR is responsible for technical administration of the contract and shall assure proper Government surveillance of the Contractor's performance. The COR shall keep a quality assurance file. At the conclusion of the contract or when requested by the CO, the COR shall provide documentation to the CO. The COR is not empowered to make any contractual commitments or to authorize any contractual changes on the Government's behalf. The Contractor shall refer any changes they deem may affect contract price, terms, or conditions to the CO for action.

c. Other Key Government Personnel - Immigration and Customs Enforcement (ICE) National Fugitive Operations Program Headquarters Staff or Federal employees as designated by the COR and/or CO.

All Point of Contact's (POC) information will be released upon award.

3. PERFORMANCE STANDARDS

Performance standards define desired services. The Contractor is responsible for performance of ALL terms and conditions of the contract. CORs will provide contract progress reports quarterly to the CO reflecting performance on this plan and all other aspects of the resultant contract. The performance standards outlined in this QASP shall be used to determine the level of Contractor performance in the elements defined.

The Government performs surveillance to determine the level of Contractor performance to these standards. Standards apply to each month of performance.

The Performance Requirements are listed below. The Government will use these standards to determine Contractor performance and shall compare Contractor performance to the standard and assign a rating. At the end of the performance period, these ratings will be used, in part, to establish the past performance of the Contractor on the contract.

The Government will use these standards to determine Contractor performance and compare Contractor performance to the Acceptable Quality Level (AQL).

Table 1: Performance Requirements Summary (PRS)

Metric	Unit of Measure	Minimum AQL
LPR Data Service	Uptime – Unit of measure 100%	> 99.0
	Operating Schedule	24/7/365
	Scheduled downtime	**</= 4 hours per month**
	Meantime between failure (MTBF)	4,000 operating hours
Overall Support Service	Support availability	24/7/365
Results of LPR Query	Result of LPR query after entered in end-user-computing device	</= 5 seconds after submission

Table 2: Performance Standards Matrix

Performance Requirement	Paragraph	Performance Standard	Performance Indicator	Performance Level	Surveillance Method	Government Documentation Criteria
LPR Data Service and Technical Support	3.0 3.1 3.2 3.3	Uptime of Data Service and Technical Support shall be fully available 24/7/365	LEIDS Data Service downtime shall not exceed 4 hours in any 1-month period and Meantime between failure (MTBF) is 4,000 operating hours	> 99.0%	Validated User/Customer Complaints 100% Inspection	Metrics will be reported in CPARS.
Overall Support Service	3.0 3.1 3.2 3.3	Support Availability	Support Service must be available 24/7/365	>99% Monitored monthly during the Transition In period.	Contractor self-monitoring and Validated User/Customer Complaints 100% Inspection	Metrics will be reported in CPARS.
Results of Query	3.2.1 3.2.2 3.2.3	Length of time for Results of LPR query to appear after being entered in the end-user computing device	Less than 5 seconds after submission	95% Monitored monthly during the life of the contract	Contractor Self-monitoring and Validated User/Customer Complaints 100% Inspection	Metrics will be reported in CPARS.

4. METHODS OF QUALITY ASSURANCE (QA) SURVEILLANCE

Regardless of the surveillance method, the COR shall always contact the Contractor's task manager or on- site representative when a defect is identified and inform the manager of the specifics of the problem. The COR, with assistance from the CO, shall be responsible for monitoring the Contractor's performance in meeting a specific performance standard/AQL.

Various methods exist to monitor performance. The COR will use the surveillance methods listed below in the administration of this QASP.

a. PERIODIC INSPECTION

- Scheduled quarterly inspection of audit logs or as required

b. VALIDATED USER/CUSTOMER COMPLAINTS

The Contractor is expected to establish and maintain professional communication between its employees and customers. The primary objective of this communication is customer satisfaction. Customer satisfaction is the most significant external indicator of the success and effectiveness of all services provided and can be measured through customer complaints.

Performance management drives the Contractor to be customer focused through initially and internally addressing customer complaints and investigating the issues and/or problems, but the customer always has the option of communicating complaints to the COR, as opposed to the Contractor.

Customer complaints, to be considered valid, must be set forth clearly and in writing the detailed nature of the complaint, must be signed, and must be forwarded to the COR.

Customer feedback may also be obtained either from the results of customer satisfaction surveys or from random customer complaints.

- Review of identified deficiencies and or complaints made by users of the services
- Investigate and validate
- Review of notification of report discrepancies

c. 100% INSPECTION

- Review of LPR Data Service uptime
- Review of Scheduled Downtime
- Review Meantime Between Failure (MTBF)
- Review Overall Support Service Availability

d. ANALYSIS OF CONTRACTOR'S PROGRESS

The Contractor is required to provide a weekly progress report that will be used to communicate the Contractor's status in the Transition phase.

e. PERFORMANCE REPORTING

Surveillance results will be used as the basis for actions against the Contractor Past Performance Report. In such cases, the Inspection of Services clause in the Contract becomes the basis for the CO's actions.

5. DOCUMENTING PERFORMANCE

Documentation must be accurate and thorough. Completeness, currency, and accuracy support both satisfactory and unsatisfactory performance

a. ACCEPTABLE PERFORMANCE

The Government shall document positive performance. All positive performance should be documented by an email to the COR describing the outstanding performance and why it is of value to the Government. This information shall become a part of the supporting documentation for the Contractor Performance Assessment Reporting System (CPARS) and the QASP

b. UNACCEPTABLE PERFORMANCE

When unacceptable performance occurs, the COR shall inform the Contractor. This will be in writing unless circumstances necessitate verbal communication. In any case the COR shall document the discussion and place it in the COR file.

When the COR determines formal written communication is required, the COR shall prepare a Contract Discrepancy Report (CDR) and present it to the Contractor's representative. A CDR template is available upon request to the Contracting Officer.

The Contractor will acknowledge receipt of the CDR in writing. The CDR will specify if the Contractor is required to prepare a corrective action plan to document how the Contractor shall correct the unacceptable performance and avoid a recurrence. The CDR will also state how long after receipt the Contractor has to present this corrective action plan to the COR. The Government shall review the Contractor's corrective action plan to determine acceptability.

Any CDRs will become a part of the supporting documentation for Past Performance.

6. FREQUENCY OF MEASUREMENT

While the Contractor is fully expected to comply with all requirements in the PWS, the Government's assessment of Contractor performance will focus mainly on the objectives listed in the AQL column of the Performance Standards Summary Matrix. The COR will monitor the Contractor's performance to ensure it meets the standards of the contract. Unacceptable performance may result in the Contracting Officer taking any of the following actions: Require the Contractor to take necessary action to ensure that future performance conforms to contract requirements, reduce the contract price to reflect the reduced value of the services, issue a Contract Discrepancy Report, or require the Contractor to re-perform the service. In addition, the Contractor's performance will be recorded annually in the Contractor Performance Assessment Report (CPAR).

Solicitation number 70CMSD21R00000002
Law Enforcement Investigative Database Subscription (LEIDS)
December 7, 2020

(i) This is a combined synopsis/solicitation issued for commercial items prepared in accordance with the format in the Federal Acquisition Regulations (FAR) Subpart 12.6, as supplemented with additional information included in this notice. This announcement constitutes the only solicitation. The clauses and provisions referenced in this solicitation may be reviewed/obtained in full text form at http://www.acquisition.gov/far.

(ii) Solicitation number 70CMSD21R00000002 is being issued using full and open competition procedures. The National American Industry Classification System (NAICS) code for this acquisition is 519130 Internet Publishing and Broadcasting and Web Search Portals, with a small business size standard of 1,000 employees. The Product Service Code (PSC) for this acquisition is D317, IT and Telecom Web Based Subscription. No set-aside will be used; however, small businesses are encouraged to submit proposals. This procurement will be conducted under FAR Part 12 supplemented with FAR Part 15 procedures. The Government anticipates awarding up to two (2) Firm Fixed Price (FFP) contracts with a one-year base period and four one-year option periods. FAR 52.217-8 Option to Extend Services will be included.

(iii) The Government will be using innovative procurement techniques for this award in order to maximize competition. Only one solicitation will be issued for the total requirement; however, the Government will be evaluating tasks separately and may or may not award two, single-award contracts as detailed below:

One contract award for all tasks—Task 1, Task 1A, Task 2, and Task 2A
Two contract awards—one award for Task 1 and Task 1A and one award for Task 2 and Task 2A

Each task would have its own technical rating. During oral presentations, each vendor would present whichever tasks they are competing for: Tasks 1 and 1A or all tasks during their allotted timeframe.

All dates included in the table below are intended to be helpful with planning purposes and are not set in stone; these dates are subject to change and may fluctuate. It is the Government's intent to adhere to this schedule.

Draft Solicitation Release	November 25, 2020
Draft Questions Due	Monday, November 30, 2020
Final Solicitation Release	December 4, 2020
Oral Presentation Request	December 11, 2020
Government conducts Oral Presentations	December 14 - 18, 2020
Government sends advisory notifications	NLT December 30, 2020
Offeror response due	NLT January 4, 2021

Phase II Submissions due	January 4, 2021
Phase II Trial Period	January 7 – 13, 2021
Award	February 16, 2021

Since the Government requested, received, and responded to questions during the draft solicitation phase, the Government may not engage in any further questions concerning this solicitation.

Phase I: Oral Presentations

Interested parties who would like to give an oral presentation to the Government must contact the Contracting Officer no later than 4:00pm CT, December 11, 2020 at (b)(6); (b)(7)(C) to secure a day/time to present a virtual oral presentation. This email request must include the offeror's participants, their role and company, and the company's expressed intent to participate in the Phase 1 Oral Presentations. Identify if presentation will cover tasks 1 and 1A or 2 and 2A or all tasks.

Offeror Participants: The Offeror's presentation team is limited to five (5) employees of the team. At least three (3) of the five (5) team members must be from the Prime Contractor. Only three (3) members of the team will present during the 90-minute technical exchange. If a Sub-contractor is included in a Prime Contractor's Oral Presentation, that Sub-contractor shall not participate in another Oral Presentation for this requirement. Sub-contractor participation in an Oral Presentation is limited to one Prime Contractor only.

Oral Presentation dates:

Oral presentations are planned between December 14-18, 2020 using Microsoft Teams. If vendors cannot access Microsoft Teams, they shall advise the contracting officer immediately so that an alternative platform can be discussed, requested, and approved prior to the oral presentation.

Oral Presentation/Demonstration Timeline for a Single Task Proposal

If an offeror is proposing to a single task (Task 1 or Task 2) and not to both tasks, the oral presentation timeline in Table 1 below will be followed.

Table 1

Oral Presentation Portion for One Task	Oral Presentation Component	Total Time Allotment (120 minutes)
1	Introductions and Rules of Engagement	Not specified
2	The Offeror will present its oral presentation/demonstration.	60 minutes
3	Window for Government to interrupt and ask questions during presentation if required for clarity	15 minutes, this will not count against the presenters 60-minute time limit
4	The Government will caucus and formulate additional question if needed.	Up to 15 minutes
5	The Government and Offeror will engage in an interactive dialogue (if needed at the sole discretion of the Government) where the Government will ask question(s) to the Offeror and the offeror responds.	Up to 30 minutes
6	The Offeror departs.	Not specified

Oral Presentation/Demonstration Timeline for a Two-Task Proposal
If an offeror is proposing under both tasks (Task 1 and Task 2), then the offeror may do so in a single oral presentation. For a two-task presentation, the oral presentation timeline in Table 2 below will be followed.

Table 2

Oral Presentation Portion for Two Tasks	Oral Presentation Component	Total Time Allotment (180 minutes)
1	Introductions and Rules of Engagement	Not specified
2	The Offeror will present its oral presentation/demonstration.	120 minute Limit**
3	Window for Government to interrupt and ask questions during presentation if required for clarity	15 minutes, this will not count against the presenters 120 minute time limit

4	The Government will caucus and formulate additional question if needed	Up to 15 minutes
5	The Government and Offeror will engage in an interactive dialogue (if needed at the sole discretion of the Government) where the Government will ask question to the Offeror and the offeror responds.	Up to 30 minutes
6	The Offeror departs.	Not specified

Oral Presentation Rules of Engagement for all Proposals

- By participating in the oral presentations, the Offeror acknowledges that it is in compliance with all solicitation rules and parameters, in accordance with applicable laws and statutes. The Government encourages Offerors to abide by applicable social distancing guidelines and rules established by the Centers for Disease Control and Prevention (CDC) and state and local Governments, including applicable active stay-at-home orders, to reduce the spread of the coronavirus disease 2019 (COVID-19).

- **Recording:** Recording of oral presentations by Offerors is strictly prohibited, notwithstanding local laws and regulations with regards to virtual meeting. The Government reserves the right to record oral presentations. If recorded, the recording is source selection sensitive and will be handled accordingly.

- Exchanges: The Government intends to engage in interactive dialogue during the oral presentations. These exchanges are viewed as a component of the oral presentation itself and do not constitute discussions. Oral presentations are distinct from the Government's reserved right to conduct clarifications or discussions.

- The Offeror participants shall not reach back, by phone/conference bridge, email or any other means, to any other personnel or persons for assistance during the oral presentation.

- Contractors will be allowed to provide handouts or other written artifacts to aid the Government in following along the presentation, however any written material must be compiled in an MS PowerPoint slide deck not exceeding 25 slides. These slides will NOT be evaluated, and any content the contractor wishes to present for an evaluation must be done orally during the oral presentation.

Advisory Notification

After the Government completes evaluation of Factor 1, Offerors will receive an advisory notification via e-mail from the Contracting Officer. This notification will advise the Offerors of the Government's advisory recommendation to proceed or not to proceed with Phase II submission. Offerors who are rated most highly for Factor 1 will be advised to

proceed to Phase II of the proposal submission process. Offerors who were not among the most highly rated will be advised that they are unlikely to be viable competitors, along with the general basis for the Government's advisory recommendation. The intent of this advice is to minimize proposal development costs for those Offerors with little to no chance of receiving an award. Offerors should note that Phase I, Factor 1 is more important than the Phase II evaluation factors.

The Government intends to provide no more than 3 Offerors with an advisory notification to proceed. However, the Government's advice will be a recommendation only, and those Offerors who are advised not to proceed may elect to continue their participation in the procurement.

Failure to participate in Phase I of the procurement precludes further consideration of an Offeror. Phase II submissions will not be accepted from Offerors who have not submitted Phase I proposals by the due date and time stated in this solicitation. For those Offerors that are rated most highly and advised to proceed to Phase II of the proposal submission process, the Contracting Officer will include the Phase II submission instructions on the advisory notification, including the date, time and exact location of the Offerors scheduled oral presentation, as well as the due date for the written portion (Price) of the Phase II submission. The Government recommends Offerors to begin preparation of Phase II proposals only after receipt of the Phase 1 advisory down-select notice.

The down-select notifications will include further information, but the Government intends to allow Offerors 48 -72 hours to decide whether it wishes to proceed with a Phase II submission. The specific times/dates for oral presentations will subsequently be provided to those Offerors remaining in Phase II.

Phase II: User Trial Period

Vendors will provide user access via a trial subscription period for up to five business days for no more than three ICE users. During this trial period vendors shall provide help desk/general user support for up to ten hours. All offerors will receive an advisory letter recommending participation/non-participation in Phase II no later than December 30, 2020. Offerors must contact the contracting officer no later than 2:00pm, Jan 4, 2021 to schedule the user trial period. Trial periods are expected to take place starting Jan 7, 2021.

The following items shall be submitted to the contracting officer no later than 4:00pm CT, January 4, 2021:

1. Solicitation Provisions and Clauses that require contractor response/fill ins.
2. Factor 3-Past Performance—submitted directly from customers to the contracting officer (using the past performance questionnaire provided by the Government).
3. Factor 4-Price Matrix—using the Price Matrix attachment provided by the Government.

NO WRITTEN/NARRATIVE PROPOSAL IS REQUIRED, NOR WILL IT BE EVALUATED IF SUBMITTED.

Estimated Total Period of Performance is 3/1/2021-2/28/2026

Contract Line Item Number	*CLIN Description*	*Quantity*	*Unit of Issue*
CLIN 0001 3/1/2021-2/28/2022	Database Functionality Requirements Task 1	12	Month
CLIN 0002 3/1/2021-2/28/2022	Training and User Maintenance Task 1A	12	Month
CLIN 0003 3/1/2021-2/28/2022	LPR Task 2	12	Month
CLIN 0004 3/1/2021-2/28/2022	LPR Training and User Maintenance Task 2A	12	Month
CLIN 1001 3/1/2022-2/28/2023	Database Functionality Requirements Task 1	12	Month
CLIN 1002 3/1/2022-2/28/2023	Training and User Maintenance Task 1A	12	Month
CLIN 1003 3/1/2022-2/28/2023	LPR Task 2	12	Month
CLIN 1004 3/1/2022-2/28/2023	LPR Training and User Maintenance Task 2A	12	Month
CLIN 2001 3/1/2023-2/28/2024	Database Functionality Requirements Task 1	12	Month
CLIN 2002 3/1/2023-2/28/2024	Training and User Maintenance Task 1A	12	Month
CLIN 2003 3/1/2023-2/28/2024	LPR Task 2	12	Month
CLIN 2004 3/1/2023-2/28/2024	LPR Training and User Maintenance Task 2A	12	Month
CLIN 3001 3/1/2024-2/28/2025	Database Functionality Requirements Task 1	12	Month
CLIN 3002 3/1/2024-2/28/2025	Training and User Maintenance Task 1A	12	Month
CLIN 3003 3/1/2024-2/28/2025	LPR Task 2	12	Month
CLIN 3004 3/1/2024-2/28/2025	LPR Training and User Maintenance Task 2A	12	Month
CLIN 4001 3/1/2025-2/28/2026	Database Functionality Requirements Task 1	12	Month
CLIN 4002 3/1/2025-2/28/2026	Training and User Maintenance Task 1A	12	Month

CLIN 4003 3/1/2025-2/28/2026	LPR Task 2	12	Month
CLIN 4004 3/1/2025-2/28/2026	LPR Training and User Maintenance Task 2A	12	Month

Description of Requirements: Contractor shall provide all personnel, supplies, and services necessary to meet the Government requirement specified in Attachment 2, Performance Work Statement (PWS) to this solicitation.

The following attachments are included for this solicitation:
Attachment 1-Clauses
Attachment 2-PWS
Attachment 3-Price Matrix
Attachment 4-Quality Assurance Surveillance Plan (QASP)
Attachment 5-Past Performance Questionnaire

FAR PROVISIONS

Provisions for this solicitation are listed below; some incorporated by reference and some included in full text. The completed provisions will not become part of the resulting IDIQ contract; they will be utilized for evaluation purposes only. The clauses listed in Attachment 1-Clauses, to this solicitation will be incorporated as an attachment to the awarded contract.

FAR Provisions Incorporated by Reference:
FAR 52.204-7, System for Award Management (Oct 2018)
FAR 52.204-16, Commercial and Government Entity Code Reporting (Jul 2016)
FAR 52.204-17, Ownership or Control of Offeror (Jul 2016)

FAR Provisions Included in Full Text:

FAR 52.204-24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (Oct 2020)

The Offeror shall not complete the representation at paragraph (d)(1) of this provision if the Offeror has represented that it "does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument" in paragraph (c)(1) in the provision at 52.204-26, Covered Telecommunications Equipment or Services—Representation, or in paragraph (v)(2)(i) of the provision at 52.212-3, Offeror Representations and Certifications-Commercial Items. The Offeror shall not complete the representation in paragraph (d)(2) of this provision if the Offeror has represented that it "does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services" in paragraph (c)(2) of the provision at 52.204-26, or in paragraph (v)(2)(ii) of the provision at 52.212-3.

(a) *Definitions.* As used in this provision—

Backhaul, covered telecommunications equipment or services, critical technology, interconnection arrangements, reasonable inquiry, roaming, and substantial or essential component have the meanings provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) *Prohibition*.

(1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Nothing in the prohibition shall be construed to—

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract or extending or renewing a contract with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract. Nothing in the prohibition shall be construed to—

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) *Procedures.* The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (https://www.sam.gov) for entities excluded from receiving federal awards for "covered telecommunications equipment or services".

(d) *Representation.* The Offeror represents that—

(1) It ☐will, ☐will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation. The Offeror shall provide the additional disclosure information required at paragraph (e)(1) of this section if the Offeror responds "will" in paragraph (d)(1) of this section; and

(2) After conducting a reasonable inquiry, for purposes of this representation, the Offeror represents that—

It ☐does, ☐does not use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services. The Offeror shall provide the additional disclosure information required at paragraph (e)(2) of this section if the Offeror responds "does" in paragraph (d)(2) of this section.

(e) *Disclosures.*

(1) Disclosure for the representation in paragraph (d)(1) of this provision. If the Offeror has responded "will" in the representation in paragraph (d)(1) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the original equipment manufacturer (OEM) or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the Product Service Code (PSC) of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(2) Disclosure for the representation in paragraph (d)(2) of this provision. If the Offeror has responded "does" in the representation in paragraph (d)(2) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the PSC of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(End of provision)

52.204-26 Covered Telecommunications Equipment or Services-Representation. (Dec 2019)

(a) *Definitions.* As used in this provision, “covered telecommunications equipment or services” has the meaning provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) *Procedures.* The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (https://www.sam.gov) for entities excluded from receiving federal awards for “covered telecommunications equipment or services”.

(c) *Representation.* The Offeror represents that it □ does, □ does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

(End of provision)

FAR 52.209-7 Information Regarding Responsibility Matters (Oct 2018)

(a) *Definitions*. As used in this provision—

"Administrative proceeding" means a non-judicial process that is adjudicatory in nature in order to make a determination of fault or liability (*e.g.*, Securities and Exchange Commission Administrative Proceedings, Civilian Board of Contract Appeals Proceedings, and Armed Services Board of Contract Appeals Proceedings). This includes administrative proceedings at the Federal and State level but only in connection with performance of a Federal contract or grant. It does not include agency actions such as contract audits, site visits, corrective plans, or inspection of deliverables.

"Federal contracts and grants with total value greater than $10,000,000" means—

(1) The total value of all current, active contracts and grants, including all priced options; and

(2) The total value of all current, active orders including all priced options under indefinite-delivery, indefinite-quantity, 8(a), or requirements contracts (including task and delivery and multiple-award Schedules).

"Principal" means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (*e.g.*, general manager; plant manager; head of a division or business segment; and similar positions).

(b) The offeror □ has □ does not have current active Federal contracts and grants with total value greater than $10,000,000.

(c)If the offeror checked "has" in paragraph (b) of this provision, the offeror represents, by submission of this offer, that the information it has entered in the Federal Awardee Performance and Integrity Information System (FAPIIS) is current, accurate, and complete as of the date of submission of this offer with regard to the following information:

(1) Whether the offeror, and/or any of its principals, has or has not, within the last five years, in connection with the award to or performance by the offeror of a Federal contract or grant, been the subject of a proceeding, at the Federal or State level that resulted in any of the following dispositions:

(i)In a criminal proceeding, a conviction.

(ii)In a civil proceeding, a finding of fault and liability that results in the payment of a monetary fine, penalty, reimbursement, restitution, or damages of $5,000 or more.

(iii)In an administrative proceeding, a finding of fault and liability that results in–

(A) The payment of a monetary fine or penalty of $5,000 or more; or

(B) The payment of a reimbursement, restitution, or damages in excess of $100,000.

(iv)In a criminal, civil, or administrative proceeding, a disposition of the matter by consent or compromise with an acknowledgment of fault by the Contractor if the proceeding could have led to any of the outcomes specified in paragraphs (c)(1)(i), (c)(1)(ii), or (c)(1)(iii) of this provision.

(2)If the offeror has been involved in the last five years in any of the occurrences listed in (c)(1) of this provision, whether the offeror has provided the requested information with regard to each occurrence.

(d) The offeror shall post the information in paragraphs (c)(1)(i) through (c)(1)(iv) of this provision in FAPIIS as required through maintaining an active registration in the System for Award Management, which can be accessed via https://www.sam.gov (see 52.204-7).

(End of provision)

FAR 52.212-1 Instructions to Offerors-Commercial Items (June 2020)

(a) *North American Industry Classification System (NAICS) code and small business size standard.* The NAICS code(s) and small business size standard(s) for this acquisition appear elsewhere in the solicitation. However, the small business size standard for a concern which submits an offer in its own name, but which proposes to furnish an item which it did not itself manufacture, is 500 employees.

(b) *Submission of offers*. Submit signed and dated offers to the office specified in this solicitation at

or before the exact time specified in this solicitation. Offers may be submitted on the SF 1449, letterhead stationery, or as otherwise specified in the solicitation. As a minimum, offers must show—

(1)The solicitation number;

(2)The time specified in the solicitation for receipt of offers;

(3)The name, address, and telephone number of the offeror;

(4)A technical description of the items being offered in sufficient detail to evaluate compliance with the requirements in the solicitation. This may include product literature, or other documents, if necessary;

(5)Terms of any express warranty;

(6)Price and any discount terms;

(7)"Remit to" address, if different than mailing address;

(8)A completed copy of the representations and certifications at FAR 52.212-3 (see FAR 52.212-3(b) for those representations and certifications that the offeror shall complete electronically);

(9)Acknowledgment of Solicitation Amendments;

(10)Past performance information, when included as an evaluation factor, to include recent and relevant contracts for the same or similar items and other references (including contract numbers, points of contact with telephone numbers and other relevant information); and

(11)If the offer is not submitted on the SF 1449, include a statement specifying the extent of agreement with all terms, conditions, and provisions included in the solicitation. Offers that fail to furnish required representations or information, or reject the terms and conditions of the solicitation may be excluded from consideration.

(c) *Period for acceptance of offers*. The offeror agrees to hold the prices in its offer firm for 30 calendar days from the date specified for receipt of offers, unless another time period is specified in an addendum to the solicitation.

(d) *Product samples*. When required by the solicitation, product samples shall be submitted at or prior to the time specified for receipt of offers. Unless otherwise specified in this solicitation, these samples shall be submitted at no expense to the Government, and returned at the sender's request and expense, unless they are destroyed during preaward testing.

(e) *Multiple offers*. Offerors are encouraged to submit multiple offers presenting alternative terms and conditions, including alternative line items (provided that the alternative line items are consistent with subpart 4.10 of the Federal Acquisition Regulation), or alternative commercial items for satisfying the requirements of this solicitation. Each offer submitted will be evaluated separately.

(f)Late submissions, modifications, revisions, and withdrawals of offers.

(1)Offerors are responsible for submitting offers, and any modifications, revisions, or withdrawals, so as to reach the Government office designated in the solicitation by the time specified in the solicitation. If no time is specified in the solicitation, the time for receipt is 4:30 p.m., local time, for the designated Government office on the date that offers or revisions are due.

(2)

(i)Any offer, modification, revision, or withdrawal of an offer received at the Government office designated in the solicitation after the exact time specified for receipt of offers is "late" and will not be considered unless it is received before award is made, the Contracting Officer determines that accepting the late offer would not unduly delay the acquisition; and-

(A)If it was transmitted through an electronic commerce method authorized by the solicitation, it was received at the initial point of entry to the Government infrastructure not later than 5:00 p.m. one working day prior to the date specified for receipt of offers; or

(B)There is acceptable evidence to establish that it was received at the Government installation designated for receipt of offers and was under the Government's control prior to the time set for receipt of offers; or

(C)If this solicitation is a request for proposals, it was the only proposal received.

(ii)However, a late modification of an otherwise successful offer, that makes its terms more favorable to the Government, will be considered at any time it is received and may be accepted.

(3)Acceptable evidence to establish the time of receipt at the Government installation includes the time/date stamp of that installation on the offer wrapper, other documentary evidence of receipt maintained by the installation, or oral testimony or statements of Government personnel.

(4)If an emergency or unanticipated event interrupts normal Government processes so that offers cannot be received at the Government office designated for receipt of offers by the exact time specified in the solicitation, and urgent Government requirements preclude amendment of the solicitation or other notice of an extension of the closing date, the time specified for receipt of offers will be deemed to be extended to the same time of day specified in the solicitation on the first work day on which normal Government processes resume.

(5)Offers may be withdrawn by written notice received at any time before the exact time set for receipt of offers. Oral offers in response to oral solicitations may be withdrawn orally. If the solicitation authorizes facsimile offers, offers may be withdrawn via facsimile received at any time before the exact time set for receipt of offers, subject to the conditions specified in the solicitation concerning facsimile offers. An offer may be withdrawn in person by an offeror or its authorized representative if, before the exact time set for receipt of offers, the identity of the person requesting withdrawal is established and the person signs a receipt for the offer.

(g) *Contract award (not applicable to Invitation for Bids*). The Government intends to evaluate offers and award a contract without discussions with offerors. Therefore, the offeror's initial offer should contain the offeror's best terms from a price and technical standpoint. However, the Government reserves the right to conduct discussions if later determined by the Contracting Officer to be necessary. The Government may reject any or all offers if such action is in the public interest; accept other than the lowest offer; and waive informalities and minor irregularities in offers received.

(h) *Multiple awards*. The Government may accept any item or group of items of an offer, unless the offeror qualifies the offer by specific limitations. Unless otherwise provided in the Schedule, offers may not be submitted for quantities less than those specified. The Government reserves the right to make an award on any item for a quantity less than the quantity offered, at the unit prices offered, unless the offeror specifies otherwise in the offer.

(i)Availability of requirements documents cited in the solicitation.

(1)

(i)The GSA Index of Federal Specifications, Standards and Commercial Item Descriptions, FPMR Part 101-29, and copies of specifications, standards, and commercial item descriptions cited in this solicitation may be obtained for a fee by submitting a request to-

GSA Federal Supply Service Specifications Section

Suite 8100 470 East L'Enfant Plaza, SW

Washington, DC 20407

Telephone (202) 619-8925

Facsimile (202) 619-8978.

(ii)If the General Services Administration, Department of Agriculture, or Department of Veterans Affairs issued this solicitation, a single copy of specifications, standards, and commercial item descriptions cited in this solicitation may be obtained free of charge by submitting a request to the addressee in paragraph (i)(1)(i) of this provision. Additional copies will be issued for a fee.

(2)Most unclassified Defense specifications and standards may be downloaded from the following ASSIST websites:

(i)ASSIST (https://assist.dla.mil/online/start/).

(ii)Quick Search (http://quicksearch.dla.mil/).

(iii)ASSISTdocs.com (http://assistdocs.com).

(3)Documents not available from ASSIST may be ordered from the Department of Defense Single Stock Point (DoDSSP) by-

(i)Using the ASSIST Shopping Wizard (https://assist.dla.mil/wizard/index.cfm);

(ii)Phoning the DoDSSP Customer Service Desk (215) 697-2179, Mon-Fri, 0730 to 1600 EST; or

(iii)Ordering from DoDSSP, Building 4, Section D, 700 Robbins Avenue, Philadelphia, PA 19111-5094, Telephone (215) 697-2667/2179, Facsimile (215) 697-1462.

(4)Nongovernment (voluntary) standards must be obtained from the organization responsible for their preparation, publication, or maintenance.

(j) *Unique entity identifier.* (Applies to all offers that exceed the micro-purchase threshold, and offers at or below the micro-purchase threshold if the solicitation requires the Contractor to be registered in the System for Award Management (SAM).) The Offeror shall enter, in the block with its name and address on the cover page of its offer, the annotation "Unique Entity Identifier" followed by the unique entity identifier that identifies the Offeror's name and address. The Offeror also shall enter its Electronic Funds Transfer (EFT) indicator, if applicable. The EFT indicator is a four-character suffix to the unique entity identifier. The suffix is assigned at the discretion of the Offeror to establish additional SAM records for identifying alternative EFT accounts (see FAR subpart 32.11) for the same entity. If the Offeror does not have a unique entity identifier, it should contact the entity designated at www.sam.gov for unique entity identifier establishment directly to obtain one. The Offeror should indicate that it is an offeror for a Government contract when contacting the entity designated at www.sam.gov for establishing the unique entity identifier.

(k)[Reserved]

(l) *Debriefing*. If a post-award debriefing is given to requesting offerors, the Government shall disclose the following information, if applicable:

(1)The agency's evaluation of the significant weak or deficient factors in the debriefed offeror's offer.

(2)The overall evaluated cost or price and technical rating of the successful and the debriefed offeror and past performance information on the debriefed offeror.

(3)The overall ranking of all offerors, when any ranking was developed by the agency during source selection.

(4)A summary of the rationale for award;

(5)For acquisitions of commercial items, the make and model of the item to be delivered by the successful offeror.

(6)Reasonable responses to relevant questions posed by the debriefed offeror as to whether source-selection procedures set forth in the solicitation, applicable regulations, and other applicable authorities were followed by the agency.

(End of provision)

FAR 52.212-2 Evaluation-Commercial Items (Oct 2014)

(a) The Government will award a contract resulting from this solicitation to the responsible offeror whose offer conforming to the solicitation will be the most advantageous to the Government, price and other factors considered. The Government will use trade off source selection procedures to procure up to two awards to the offeror(s) whose solution(s) represents the best value to the Government. The Government may award to other than the lowest priced or the highest rated offeror(s). The evaluation will be conducted as a two phase, advisory down select. The phases will include the following evaluation factors:

Phase I
Factor 1: Technical Approach (Demonstration/Oral Presentation)

Phase II
Factor 2: Trial Test Period for Subject Matter Experts (SMEs)
Factor 3: Past Performance
Factor 4: Price

The order of importance is as follows:

The factors are listed in descending order of importance: Factor 1, 2, 3, and 4. When all technical factors are combined, they are significantly more important than price. Factor 4, Price, is the least important factor.

(b) *Options*. The Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. The Government may determine that an offer is unacceptable if the option prices are significantly unbalanced. Evaluation of options shall not obligate the Government to exercise the option(s).

(c)A written notice of award or acceptance of an offer, mailed or otherwise furnished to the successful offeror within the time for acceptance specified in the offer, shall result in a binding contract without further action by either party. Before the offer's specified expiration time, the Government may accept an offer (or part of an offer), whether or not there are negotiations after its receipt, unless a written notice of withdrawal is received before award.

(End of provision)

Rating Scale for Technical Factors 1 and 2

In evaluating Factors 1 and 2, each factor will have its own confidence assessment. The Government will consider the Offeror's approaches and the risks associated with the approaches proposed by the Offeror to arrive at a confidence assessment of the Offeror's likelihood of successfully performing the work. The table below shows the ratings the Government will assign in its evaluation of these factors.

Technical Evaluation Confidence Ratings	
Rating	**Definition**
High Confidence	The Government has *high confidence* that the Offeror understands the requirement, proposes a sound approach, and will be successful in performing the contract with *little or no* Government intervention.
Some Confidence	The Government has *some confidence* that the Offeror understands the requirement, proposes a sound approach, and will be successful in performing the contract with *some* Government intervention.
Low Confidence	The Government has *low confidence* that the Offeror understands the requirement, proposes a sound approach, and will be successful in performing the contract *even with* Government intervention.

Phase I

Factor 1, Technical Approach (Demonstration/Oral Presentation)
Factor 1 will be evaluated by Offerors providing an oral presentation to the Government's technical team. This presentation will be done via MS Teams. Each offeror should cover the requirements under PWS, Section 3.0 Task Requirements during their presentation.

Advisory Down Select

Phase II

Factor 2, Trial Test Period for SMEs
Factor 2 will be evaluated through a five-day (business) trial/test period for SMEs. During this time, each contractor shall provide up to ten hours of help desk or instructional support for the SMEs. This support may be via telephone or email. The Government will assess its confidence that the offeror will be successful in performing the contract based on its Factor 2 Trial Test Period. The testing includes, but is not limited to:

1. User friendliness
2. Effectiveness and response time of help desk support
3. Ability to run specific reports/details within each report available
4. Validity of data received during trial period

Offerors may be rated more highly if their database has unique or added features, or other innovations, that provide benefit to the Government. It is possible that an offeror's database offers additional features that are of no additional benefit to the Government. Those features will not assist offerors in getting a higher confidence rating for this factor. The determination of what features are of benefit to the Government is at the sole discretion of the Government and its evaluation team.

Factor 3: Past Performance

The Government is providing a "Contractor Past Performance Evaluation Survey" (RFP Past Performance

Attachment) for Offerors to submit to the cited client/customer points of contact for completion. The completed survey forms must be returned directly to Tracy Riley no later than the first day of the trial/test period in Phase II. Client can email surveys to Tracy.Riley@ice.dhs.gov. The completed survey must come from the Client (not the Offeror). The Offeror is responsible for ensuring timely submission. The Government is seeking to determine whether the Offeror has a high-quality record of past performance that will enhance its ability to successfully perform the required effort. Past Performance should be recent and relevant. No past performance on contracts that ended more than three years ago will be accepted. Similarly, contracts that are not of similar size and scope will not be accepted.

In evaluating past performance, the Government may supplement the information offerors provide with performance information it may obtain from any source including its own experience with the offeror performing prior orders with the federal Government or otherwise, and agency databases.

The Government, after reviewing the past performance information, will assign a confidence rating rating of "High Confidence", "Some Confidence", "Low Confidence", or "Unknown Confidence/N/A" to Factor 3, Past Performance.

Past Performance Rating Definitions:

High Confidence
Based on the Offeror's recent (NLT 3 years) and relevant (similar in magnitude and scope of this effort) performance record, the Government has a high expectation that the Offeror will successfully perform based on the offeror's performance.

Some Confidence
Based on the Offeror's recent (NLT 3 years) and relevant (similar in magnitude and scope of this effort) performance record, the Government has a reasonable expectation that the Offeror will successfully perform based on the offeror's performance.

Low Confidence
Based on the Offeror's recent (NLT 3 years) and relevant (similar in magnitude and scope of this effort) performance record, the Government has a limited expectation that the Offeror will successfully perform based on the offeror's performance.

Unknown Confidence (N/A)
The Offeror does not have recent (NLT 3 years) and relevant (similar in magnitude and scope of this effort) performance; or the Offeror's performance record is so sparse, a meaningful confidence rating cannot be reasonably assigned. This rating is neutral, neither favorable or unfavorable.

Factor 4: Price:

Offerors do not need submit pricing until Phase II. If an offeror decides they do not wish to participate in Phase II, no pricing will be required from that offeror. The Government will provide a price matrix with this solicitation for all offerors to fill out. The matrix will be

broken down by task.

Price will be evaluated to determine whether it is fair and reasonable. Price will be evaluated by CLIN/Task Number. Each offeror shall propose pricing for the task(s) they plan to compete for. For example, if a company plans to compete for both tasks, that offeror shall submit pricing for each task separately; in a second column in the price matrix will contain pricing for each task assuming an offeror were to win both tasks (only one contract award made). This allows offerors to provide any discounts that would be provided if an offeror were to be awarded both tasks.

The Government will evaluate price on Offerors' Total Evaluated Price (TEP). The TEP by adding the base and all option years for the total period of performance to include the possible six-month extension IAW FAR 52.217-8 Option to Extend Services. There will not be a separate CLIN for the possible extension (up to six months) at the end of Option Period Four. Offerors do not need to submit pricing for FAR 52.217-8. The Government will use the pricing submitted for Option Period Four to calculate the pricing for the possible six-month extension for evaluation purposes. If Option Period Four is extended the period of performance for that option will simply be extended, at the same prices.

FAR 52.212-3 Offeror Representations and Certifications-Commercial Items (Dec 2019)
Offeror Representations and Certifications-Commercial Items (Nov 2020)
The Offeror shall complete only paragraph (b) of this provision if the Offeror has completed the annual representations and certification electronically in the System for Award Management (SAM) accessed through https://www.sam.gov. If the Offeror has not completed the annual representations and certifications electronically, the Offeror shall complete only paragraphs (c) through (v)) of this provision.

(a) *Definitions*. As used in this provision—

"Covered telecommunications equipment or services" has the meaning provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

Economically disadvantaged women-owned small business (EDWOSB) concern means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States and who are economically disadvantaged in accordance with 13 CFR part 127. It automatically qualifies as a women-owned small business eligible under the WOSB Program.

Forced or indentured child labor means all work or service—

(1) Exacted from any person under the age of 18 under the menace of any penalty for its nonperformance and for which the worker does not offer himself voluntarily; or

(2) Performed by any person under the age of 18 pursuant to a contract the enforcement of which can be accomplished by process or penalties.

Highest-level owner means the entity that owns or controls an immediate owner of the offeror, or that owns or controls one or more entities that control an immediate owner of the offeror. No entity owns or exercises control of the highest level owner.

Immediate owner means an entity, other than the offeror, that has direct control of the offeror. Indicators of control include, but are not limited to, one or more of the following: ownership or interlocking

management, identity of interests among family members, shared facilities and equipment, and the common use of employees.

Inverted domestic corporation, means a foreign incorporated entity that meets the definition of an inverted domestic corporation under 6 U.S.C. 395(b), applied in accordance with the rules and definitions of 6 U.S.C. 395(c).

Manufactured end product means any end product in product and service codes (PSCs) 1000-9999, except—

(1) PSC 5510, Lumber and Related Basic Wood Materials;
(2) Product or Service Group (PSG) 87, Agricultural Supplies;
(3) PSG 88, Live Animals;
(4) PSG 89, Subsistence;
(5) PSC 9410, Crude Grades of Plant Materials;
(6) PSC 9430, Miscellaneous Crude Animal Products, Inedible;
(7) PSC 9440, Miscellaneous Crude Agricultural and Forestry Products;
(8) PSC 9610, Ores;
(9) PSC 9620, Minerals, Natural and Synthetic; and
(10) PSC 9630, Additive Metal Materials.

Place of manufacture means the place where an end product is assembled out of components, or otherwise made or processed from raw materials into the finished product that is to be provided to the Government. If a product is disassembled and reassembled, the place of reassembly is not the place of manufacture.

Place of manufacture means the place where an end product is assembled out of components, or otherwise made or processed from raw materials into the finished product that is to be provided to the Government. If a product is disassembled and reassembled, the place of reassembly is not the place of manufacture.

Predecessor means an entity that is replaced by a successor and includes any predecessors of the predecessor.

Reasonable inquiry has the meaning provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

Restricted business operations means business operations in Sudan that include power production activities, mineral extraction activities, oil-related activities, or the production of military equipment, as those terms are defined in the Sudan Accountability and Divestment Act of 2007 (Pub. L. 110-174). Restricted business operations do not include business operations that the person (as that term is defined in Section 2 of the Sudan Accountability and Divestment Act of 2007) conducting the business can demonstrate—

(1) Are conducted under contract directly and exclusively with the regional government of southern Sudan;

(2) Are conducted pursuant to specific authorization from the Office of Foreign Assets Control in the Department of the Treasury, or are expressly exempted under Federal law from the requirement to be conducted under such authorization;

(3) Consist of providing goods or services to marginalized populations of Sudan;

(4) Consist of providing goods or services to an internationally recognized peacekeeping force or humanitarian organization;

(5) Consist of providing goods or services that are used only to promote health or education; or

(6) Have been voluntarily suspended. "Sensitive technology"—

Sensitive technology—

(1) Means hardware, software, telecommunications equipment, or any other technology that is to be used specifically—

(i) To restrict the free flow of unbiased information in Iran; or

(ii) To disrupt, monitor, or otherwise restrict speech of the people of Iran; and

(2) Does not include information or informational materials the export of which the President does not have the authority to regulate or prohibit pursuant to section 203(b)(3)of the International Emergency Economic Powers Act (50 U.S.C. 1702(b)(3)).

Service-disabled veteran-owned small business concern—

(1) Means a small business concern—

(i) Not less than 51 percent of which is owned by one or more service-disabled veterans or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more service-disabled veterans; and

(ii) The management and daily business operations of which are controlled by one or more service-disabled veterans or, in the case of a service-disabled veteran with permanent and severe disability, the spouse or permanent caregiver of such veteran.

(2) Service-disabled veteran means a veteran, as defined in 38 U.S.C. 101(2), with a disability that is service connected, as defined in 38 U.S.C. 101(16).

Small business concern—

(1) Means a concern, including its affiliates, that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the criteria in 13 CFR part 121 and size standards in this solicitation.

(2) *Affiliates*, as used in this definition, means business concerns, one of whom directly or indirectly controls or has the power to control the others, or a third party or parties control or have the power to control the others. In determining whether affiliation exists, consideration is given to all appropriate factors including common ownership, common management, and contractual relationships. SBA determines affiliation based on the factors set forth at 13 CFR 121.103.

Small disadvantaged business concern, consistent with13 CFR 124.1002, means a small business concern under the size standard applicable to the acquisition, that—

(1) Is at least 51 percent unconditionally and directly owned (as defined at 13 CFR 124.105) by—(i) One or more socially disadvantaged (as defined at13 CFR 124.103) and economically disadvantaged (as defined at 13 CFR 124.104) individuals who are citizens of the United States; and

(ii) Each individual claiming economic disadvantage has a net worth not exceeding $750,000 after taking into account the applicable exclusions set forth at 13 CFR124.104(c)(2); and

(2) The management and daily business operations of which are controlled (as defined at 13.CFR 124.106) by individuals, who meet the criteria in paragraphs (1)(i) and (ii) of this definition.

Subsidiary means an entity in which more than 50 percent of the entity is owned—

(1) Directly by a parent corporation; or

(2) Through another subsidiary of a parent corporation

Successor means an entity that has replaced a predecessor by acquiring the assets and carrying out the affairs of the predecessor under a new name (often through acquisition or merger). The term "successor" does not include new offices/divisions of the same company or a company that only changes its name. The extent of the responsibility of the successor for the liabilities of the predecessor may vary, depending on State law and specific circumstances.

Veteran-owned small business concern means a small business concern—

(1) Not less than 51 percent of which is owned by one or more veterans (as defined at 38 U.S.C. 101(2)) or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more veterans; and
(2) The management and daily business operations of which are controlled by one or more veterans.

Women-owned small business (WOSB) concern eligible under the WOSB Program (in accordance with 13 CFR part 127), means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States.

Women-owned small business concern means a small business concern—

(1) That is at least 51 percent owned by one or more women; or, in the case of any publicly owned business, at least51 percent of the stock of which is owned by one or more women; and

(2) Whose management and daily business operations are controlled by one or more women.

(b)
(1) *Annual Representations and Certifications*. Any changes provided by the Offeror in paragraph (b)(2) of this provision do not automatically change the representations and certifications in SAM

(2) The offeror has completed the annual representations and certifications electronically in SAM accessed through http://www.sam.gov. After reviewing SAM information, the Offeror verifies by submission of this offer that the representations and certifications currently posted electronically at FAR 52.212-3, Offeror Representations and Certifications-Commercial Items, have been entered or updated in the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard(s) applicable to the NAICS code(s) referenced for this solicitation), at the time this offer is submitted and are incorporated in this offer by reference (see FAR 4.1201), except for paragraphs _____.

[*Offeror to identify the applicable paragraphs at (c) through (v) of this provision that the offeror has completed for the purposes of this solicitation only, if any.*

These amended representation(s) and/or certification(s) are also incorporated in this offer and are current, accurate, and complete as of the date of this offer.

Any changes provided by the offeror are applicable to this solicitation only, and do not result in an update to the representations and certifications posted electronically on SAM.]

(c) Offerors must complete the following representations when the resulting contract will be performed in the United States or its outlying areas. Check all that apply.

(1) *Small business concern*. The offeror represents as part of its offer that it □ is, □ is not a small business concern.

(2) *Veteran-owned small business concern*. [*Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision*.] The offeror represents as part of its offer that it □ is, □ is not a veteran-owned small business concern.

(3) *Service-disabled veteran-owned small business concern*. [*Complete only if the offeror represented itself as a veteran-owned small business concern in paragraph (c)(2) of this provision*.] The offeror represents as part of its offer that it □ is, □ is not a service-disabled veteran-owned small business concern.

(4) *Small disadvantaged business concern*. [*Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision*.] The offeror represents, that it □ is, □ is not a small disadvantaged business concern as defined in 13 CFR124.1002.

(5) *Women-owned small business concern*. [*Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision*.] The offeror represents that it □ is, □ is not a women-owned small business concern.

(6) WOSB concern eligible under the WOSB Program. [Complete only if the offeror represented itself as a women-owned small business concern in paragraph (c)(5) of this provision.] The offeror represents that-

(i) It □ is, □ is not a WOSB concern eligible under the WOSB Program, has provided all the required documents to the WOSB Repository, and no change in circumstances or adverse decisions have been issued that affects its eligibility; and

(ii) It □ is, □ is not a joint venture that complies with the requirements of 13 CFR part 127, and the representation in paragraph (c)(6)(i) of this provision is accurate for each WOSB concern eligible under the WOSB Program participating in the joint venture. [The offeror shall enter the name or names of the WOSB concern eligible under the WOSB Program and other small businesses that are participating in the joint venture: _____.] Each WOSB concern eligible under the WOSB Program participating in the joint venture shall submit a separate signed copy of the WOSB representation.

(7) Economically disadvantaged women-owned small business (EDWOSB) concern. [Complete only if the offeror represented itself as a WOSB concern eligible under the WOSB Program in (c)(6) of this provision.] The offeror represents that-

(i) It □ is, □ is not an EDWOSB concern, has provided all the required documents to the WOSB Repository, and no change in circumstances or adverse decisions have been issued that affects its eligibility; and

(ii) It □ is, □ is not a joint venture that complies with the requirements of 13 CFR part 127, and the representation in paragraph (c)(7)(i) of this provision is accurate for each EDWOSB concern participating in the joint venture. [*The offeror shall enter the name or names of the EDWOSB concern and other small businesses that are participating in the joint venture:* _____.] Each EDWOSB concern participating in the joint venture shall submit a separate signed copy of the EDWOSB representation.

Note: Complete paragraphs (c)(8) and (c)(9) only if this solicitation is expected to exceed the simplified acquisition threshold.

(8) *Women-owned business concern (other than small business concern*). [*Complete only if the offeror is a women-owned business concern and did not represent itself as a small business concern in paragraph (c)(1) of this provision*.] The offeror represents that it □ is a women-owned business concern.

(9) *Tie bid priority for labor surplus area concerns*. If this is an invitation for bid, small business offerors may identify the labor surplus areas in which costs to be incurred on account of manufacturing or production (by offeror or first-tier subcontractors) amount to more than 50 percent of the contract price:_____

(10) *HUBZone small business concern*. [*Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision*.] The offeror represents, as part of its offer, that–

(i) It □ is, □ is not a HUBZone small business concern listed, on the date of this representation, on the List of Qualified HUBZone Small Business Concerns maintained by the Small Business Administration, and no material changes in ownership and control, principal office, or HUBZone employee percentage have occurred since it was certified in accordance with 13 CFR Part 126; and

(ii) It □ is, □ is not a HUBZone joint venture that complies with the requirements of 13 CFR Part 126, and the representation in paragraph (c)(10)(i) of this provision is accurate for each HUBZone small business concern participating in the HUBZone joint venture. [The offeror shall enter the names of each of the HUBZone small business concerns participating in the HUBZone joint venture: _____.] Each

HUBZone small business concern participating in the HUBZone joint venture shall submit a separate signed copy of the HUBZone representation.

(d) Representations required to implement provisions of Executive Order11246-

(1) Previous contracts and compliance. The offeror represents that-

(i) It □ has, □ has not participated in a previous contract or subcontract subject to the Equal Opportunity clause of this solicitation; and

(ii) It □ has, □ has not filed all required compliance reports.

(2) *Affirmative Action Compliance*. The offeror represents that-

(i) It □ has developed and has on file, □ has not developed and does not have on file, at each establishment, affirmative action programs required by rules and regulations of the Secretary of Labor (41 CFR parts 60-1 and 60-2), or

(ii) It □ has not previously had contracts subject to the written affirmative action programs requirement of the rules and regulations of the Secretary of Labor.

(e) *Certification Regarding Payments to Influence Federal Transactions (31 http://uscode.house.gov/ U.S.C. 1352)*. (Applies only if the contract is expected to exceed $150,000.) By submission of its offer, the offeror certifies to the best of its knowledge and belief that no Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress or an employee of a Member of Congress on his or her behalf in connection with the award of any resultant contract. If any registrants under the Lobbying Disclosure Act of 1995 have made a lobbying contact on behalf of the offeror with respect to this contract, the offeror shall complete and submit, with its offer, OMB Standard Form LLL, Disclosure of Lobbying Activities, to provide the name of the registrants. The offeror need not report regularly employed officers or employees of the offeror to whom payments of reasonable compensation were made.

(f) *Buy American Certificate*. (Applies only if the clause at Federal Acquisition Regulation (FAR) 52.225-1, Buy American-Supplies, is included in this solicitation.)

(1) The offeror certifies that each end product, except those listed in paragraph (f)(2) of this provision, is a domestic end product and that for other than COTS items, the offeror has considered components of unknown origin to have been mined, produced, or manufactured outside the United States. The offeror shall list as foreign end products those end products manufactured in the United States that do not qualify as domestic end products, *i.e.*, an end product that is not a COTS item and does not meet the component test in paragraph (2) of the definition of "domestic end product." The terms "commercially available off-the-shelf (COTS) item" "component," "domestic end product," "end product," "foreign end product," and "United States" are defined in the clause of this solicitation entitled "Buy American-Supplies."

(2) Foreign End Products:

Line Item No.	**Country of Origin**
_____	_____
_____	_____
_____	_____

[*List as necessary*]

(3) The Government will evaluate offers in accordance with the policies and procedures of FAR part 25.

(g)

(1) *Buy American-Free Trade Agreements-Israeli Trade Act Certificate*. (Applies only if the clause at FAR 52.225-3, Buy American-Free Trade Agreements-Israeli Trade Act, is included in this solicitation.)
(i) The offeror certifies that each end product, except those listed in paragraph (g)(1)(ii) or (g)(1)(iii) of this provision, is a domestic end product and that for other than COTS items, the offeror has considered components of unknown origin to have been mined, produced, or manufactured outside the United States. The terms "Bahrainian, Moroccan, Omani, Panamanian, or Peruvian end product," "commercially available off-the-shelf (COTS) item," "component," "domestic end product," "end product," "foreign end product," "Free Trade Agreement country," "Free Trade Agreement country end product," "Israeli end product," and "United States" are defined in the clause of this solicitation entitled "Buy American-Free Trade Agreements–Israeli Trade Act."

(ii) The offeror certifies that the following supplies are Free Trade Agreement country end products (other than Bahrainian, Moroccan, Omani, Panamanian, or Peruvian end products) or Israeli end products as defined in the clause of this solicitation entitled "Buy American-Free Trade Agreements-Israeli Trade Act":

Free Trade Agreement Country End Products (Other than Bahrainian, Moroccan, Omani, Panamanian, or Peruvian End Products) or Israeli End Products:

Line Item No.	**Country of Origin**
_____	_____
_____	_____
_____	_____

[*List as necessary*]

(iii) The offeror shall list those supplies that are foreign end products (other than those listed in paragraph (g)(1)(ii) of this provision) as defined in the clause of this solicitation entitled "Buy American-Free Trade Agreements-Israeli Trade Act." The offeror shall list as other foreign end products those end products manufactured in the United States that do not qualify as domestic end products, *i.e.*, an end product that is not a COTS item and does not meet the component test in paragraph (2) of the definition of "domestic end product."

Other Foreign End Products:

Line Item No.	**Country of Origin**
_____	_____
_____	_____
_____	_____

[List as necessary]

(iv) The Government will evaluate offers in accordance with the policies and procedures of FAR part 25.

(2) *Buy American-Free Trade Agreements-Israeli Trade Act Certificate, Alternate I*. If Alternate I to the clause at FAR 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

(g)(1)(ii) The offeror certifies that the following supplies are Canadian end products as defined in the clause of this solicitation entitled "Buy American-Free Trade Agreements-Israeli Trade Act":

Canadian End Products:

Line Item No.

_____

_____

_____

[*List as necessary*]

(3) *Buy American-Free Trade Agreements-Israeli Trade Act Certificate, Alternate II*. If Alternate II to the clause at FAR 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

(g)(1)(ii) The offeror certifies that the following supplies are Canadian end products or Israeli end products as defined in the clause of this solicitation entitled "Buy American-Free Trade Agreements-Israeli Trade Act":

Canadian or Israeli End Products:

Line Item No.	Country of Origin
_____	_____
_____	_____
_____	_____

[*List as necessary*]

(4) *Buy American-Free Trade Agreements-Israeli Trade Act Certificate, Alternate III*. If Alternate III to the clause at 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

(g)(1)(ii) The offeror certifies that the following supplies are Free Trade Agreement country end products (other than Bahrainian, Korean, Moroccan, Omani, Panamanian, or Peruvian end products) or Israeli end products as defined in the clause of this solicitation entitled "Buy American-Free Trade Agreements-Israeli Trade Act":

Free Trade Agreement Country End Products (Other than Bahrainian, Korean, Moroccan, Omani, Panamanian, or Peruvian End Products) or Israeli End Products:

Line Item No.	Country of Origin
_____	_____
_____	_____
_____	_____

[*List as necessary*]

(5) *Trade Agreements Certificate*. (Applies only if the clause at FAR 52.225-5, Trade Agreements, is included in this solicitation.)

(i) The offeror certifies that each end product, except those listed in paragraph (g)(5)(ii) of this provision, is a U.S.-made or designated country end product, as defined in the clause of this solicitation entitled "Trade Agreements."

(ii) The offeror shall list as other end products those end products that are not U.S.-made or designated country end products.

Other End Products:

Line Item No.	Country of Origin
_____	_____

Line Item No.	Country of Origin
_____	_____
_____	_____

[*List as necessary*]

(iii) The Government will evaluate offers in accordance with the policies and procedures of FAR part 25. For line items covered by the WTO GPA, the Government will evaluate offers of U.S.-made or designated country end products without regard to the restrictions of the Buy American statute. The Government will consider for award only offers of U.S.-made or designated country end products unless the Contracting Officer determines that there are no offers for such products or that the offers for such products are insufficient to fulfill the requirements of the solicitation.

(h) *Certification Regarding Responsibility Matters (Executive Order 12689*). (Applies only if the contract value is expected to exceed the simplified acquisition threshold.) The offeror certifies, to the best of its knowledge and belief, that the offeror and/or any of its principals–

(1) □ Are, □ are not presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency;

(2) □ Have, □ have not, within a three-year period preceding this offer, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a Federal, state or local government contract or subcontract; violation of Federal or state antitrust statutes relating to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, violating Federal criminal tax laws, or receiving stolen property;

(3) □ Are, □ are not presently indicted for, or otherwise criminally or civilly charged by a Government entity with, commission of any of these offenses enumerated in paragraph (h)(2) of this clause; and

(4) □ Have, □ have not, within a three-year period preceding this offer, been notified of any delinquent Federal taxes in an amount that exceeds the threshold at 9.104-5(a)(2) for which the liability remains unsatisfied.

(i) Taxes are considered delinquent if both of the following criteria apply:

(A) *The tax liability is finally determined*. The liability is finally determined if it has been assessed. A liability is not finally determined if there is a pending administrative or judicial challenge. In the case of a judicial challenge to the liability, the liability is not finally determined until all judicial appeal rights have been exhausted.

(B) *The taxpayer is delinquent in making payment*. A taxpayer is delinquent if the taxpayer has failed to pay the tax liability when full payment was due and required. A taxpayer is not delinquent in cases where enforced collection action is precluded.

(ii) *Examples*.

(A) The taxpayer has received a statutory notice of deficiency, under I.R.C. §6212, which entitles the taxpayer to seek Tax Court review of a proposed tax deficiency. This is not a delinquent tax because it is not a final tax liability. Should the taxpayer seek Tax Court review, this will not be a final tax liability until the taxpayer has exercised all judicial appeal rights.

(B) The IRS has filed a notice of Federal tax lien with respect to an assessed tax liability, and the taxpayer has been issued a notice under I.R.C. §6320 entitling the taxpayer to request a hearing with the IRS Office of Appeals contesting the lien filing, and to further appeal to the Tax Court if the IRS determines to sustain the lien filing. In the course of the hearing, the taxpayer is entitled to contest the

underlying tax liability because the taxpayer has had no prior opportunity to contest the liability. This is not a delinquent tax because it is not a final tax liability. Should the taxpayer seek tax court review, this will not be a final tax liability until the taxpayer has exercised all judicial appeal rights.

(C) The taxpayer has entered into an installment agreement pursuant to I.R.C. §6159. The taxpayer is making timely payments and is in full compliance with the agreement terms. The taxpayer is not delinquent because the taxpayer is not currently required to make full payment.

(D) The taxpayer has filed for bankruptcy protection. The taxpayer is not delinquent because enforced collection action is stayed under 11 U.S.C. §362 (the Bankruptcy Code).

(i) *Certification Regarding Knowledge of Child Labor for Listed End Products (Executive Order 13126). [The Contracting Officer must list in paragraph (i)(1) any end products being acquired under this solicitation that are included in the List of Products Requiring Contractor Certification as to Forced or Indentured Child Labor, unless excluded at 22.1503(b).]*

(1) *Listed end products.*

Listed End Product	**Listed Countries of Origin**
_____	_____
_____	_____

(2) *Certification. [If the Contracting Officer has identified end products and countries of origin in paragraph (i)(1) of this provision, then the offeror must certify to either (i)(2)(i) or (i)(2)(ii) by checking the appropriate block.]*

(i) The offeror will not supply any end product listed in paragraph (i)(1) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product.

(ii) The offeror may supply an end product listed in paragraph (i)(1) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product. The offeror certifies that it has made a good faith effort to determine whether forced or indentured child labor was used to mine, produce, or manufacture any such end product furnished under this contract. On the basis of those efforts, the offeror certifies that it is not aware of any such use of child labor.

(j) *Place of manufacture.* (Does not apply unless the solicitation is predominantly for the acquisition of manufactured end products.) For statistical purposes only, the offeror shall indicate whether the place of manufacture of the end products it expects to provide in response to this solicitation is predominantly-

(1) □ In the United States (Check this box if the total anticipated price of offered end products manufactured in the United States exceeds the total anticipated price of offered end products manufactured outside the United States); or

(2) □ Outside the United States.

(k) *Certificates regarding exemptions from the application of the Service Contract Labor Standards* (Certification by the offeror as to its compliance with respect to the contract also constitutes its certification as to compliance by its subcontractor if it subcontracts out the exempt services.) [*The contracting officer is to check a box to indicate if paragraph (k)(1) or (k)(2) applies.*]

(1) Maintenance, calibration, or repair of certain equipment as described in FAR 22.1003-4(c)(1). The offeror □ does □ does not certify that–

(i) The items of equipment to be serviced under this contract are used regularly for other than Governmental purposes and are sold or traded by the offeror (or subcontractor in the case of an exempt subcontract) in substantial quantities to the general public in the course of normal business operations;

(ii) The services will be furnished at prices which are, or are based on, established catalog or market prices (see FAR 22.1003-4(c)(2)(ii)) for the maintenance, calibration, or repair of such equipment; and

(iii) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract will be the same as that used for these employees and equivalent employees servicing the same equipment of commercial customers.

(2) Certain services as described in FAR 22.1003-4(d)(1). The offeror □ does □ does not certify that-

(i) The services under the contract are offered and sold regularly to non-Governmental customers, and are provided by the offeror (or subcontractor in the case of an exempt subcontract) to the general public in substantial quantities in the course of normal business operations;

(ii) The contract services will be furnished at prices that are, or are based on, established catalog or market prices (see FAR 22.1003-4(d)(2)(iii));

(iii) Each service employee who will perform the services under the contract will spend only a small portion of his or her time (a monthly average of less than 20 percent of the available hours on an annualized basis, or less than 20 percent of available hours during the contract period if the contract period is less than a month) servicing the Government contract; and

(iv) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract is the same as that used for these employees and equivalent employees servicing commercial customers.

(3) If paragraph (k)(1) or (k)(2) of this clause applies–

(i) If the offeror does not certify to the conditions in paragraph (k)(1) or (k)(2) and the Contracting Officer did not attach a Service Contract Labor Standards wage determination to the solicitation, the offeror shall notify the Contracting Officer as soon as possible; and

(ii) The Contracting Officer may not make an award to the offeror if the offeror fails to execute the certification in paragraph (k)(1) or (k)(2) of this clause or to contact the Contracting Officer as required in paragraph (k)(3)(i) of this clause.

(l) *Taxpayer Identification Number (TIN) (* 26 U.S.C. 6109, 31 U.S.C. 7701). (Not applicable if the offeror is required to provide this information to the SAM to be eligible for award.)

(1) All offerors must submit the information required in paragraphs (l)(3) through (l)(5) of this provision to comply with debt collection requirements of 31 U.S.C. 7701(c) and 3325(d), reporting requirements of 26 U.S.C. 6041, 6041A, and 6050M, and implementing regulations issued by the Internal Revenue Service (IRS).

(2) The TIN may be used by the Government to collect and report on any delinquent amounts arising out of the offeror's relationship with the Government (31 U.S.C. 7701(c)(3)). If the resulting contract is subject to the payment reporting requirements described in FAR 4.904, the TIN provided hereunder may be matched with IRS records to verify the accuracy of the offeror's TIN.

(3) *Taxpayer Identification Number (TIN).*

TIN: _____.

TIN has been applied for.

TIN is not required because:

Offeror is a nonresident alien, foreign corporation, or foreign partnership that does not have income effectively connected with the conduct of a trade or business in the United States and does not have an office or place of business or a fiscal paying agent in the United States;

Offeror is an agency or instrumentality of a foreign government;

Offeror is an agency or instrumentality of the Federal Government.

(4) *Type of organization*.

Sole proprietorship;
Partnership;
Corporate entity (not tax-exempt);
Corporate entity (tax-exempt);
Government entity (Federal, State, or local);
Foreign government;
International organization per 26 CFR1.6049-4;
Other _____.

(5) *Common parent*.

Offeror is not owned or controlled by a common parent;
Name and TIN of common parent:

Name _____.
TIN _____.

(m) *Restricted business operations in Sudan*. By submission of its offer, the offeror certifies that the offeror does not conduct any restricted business operations in Sudan.

(n) Prohibition on Contracting with Inverted Domestic Corporations.

(1) Government agencies are not permitted to use appropriated (or otherwise made available) funds for contracts with either an inverted domestic corporation, or a subsidiary of an inverted domestic corporation, unless the exception at 9.108-2(b) applies or the requirement is waived in accordance with the procedures at 9.108-4.

(2) *Representation*. The Offeror represents that–

(i) It □ is, □ is not an inverted domestic corporation; and

(ii) It □ is, □ is not a subsidiary of an inverted domestic corporation.

(o) Prohibition on contracting with entities engaging in certain activities or transactions relating to Iran.

(1) The offeror shall e-mail questions concerning sensitive technology to the Department of State at CISADA106@state.gov.

(2) *Representation and Certifications*. Unless a waiver is granted or an exception applies as provided in paragraph (o)(3) of this provision, by submission of its offer, the offeror-

(i) Represents, to the best of its knowledge and belief, that the offeror does not export any sensitive technology to the government of Iran or any entities or individuals owned or controlled by, or acting on behalf or at the direction of, the government of Iran;

(ii) Certifies that the offeror, or any person owned or controlled by the offeror, does not engage in any activities for which sanctions may be imposed under section 5 of the Iran Sanctions Act; and

(iii) Certifies that the offeror, and any person owned or controlled by the offeror, does not knowingly engage in any transaction that exceeds the threshold at FAR 25.703-2(a)(2) with Iran's Revolutionary Guard Corps or any of its officials, agents, or affiliates, the property and interests in property of which are blocked pursuant to the International Emergency Economic Powers Act (et seq.) (see OFAC's Specially Designated Nationals and Blocked Persons List at https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx).

(3) The representation and certification requirements of paragraph (o)(2) of this provision do not apply if-

(i) This solicitation includes a trade agreements certification (*e.g.*, 52.212-3(g) or a comparable agency provision); and

(ii) The offeror has certified that all the offered products to be supplied are designated country end products.

(p) *Ownership or Control of Offeror*. (Applies in all solicitations when there is a requirement to be registered in SAM or a requirement to have a unique entity identifier in the solicitation).

(1) The Offeror represents that it □ has or □ does not have an immediate owner. If the Offeror has more than one immediate owner (such as a joint venture), then the Offeror shall respond to paragraph (2) and if applicable, paragraph (3) of this provision for each participant in the joint venture.

(2) If the Offeror indicates "has" in paragraph (p)(1) of this provision, enter the following information:

Immediate owner CAGE code: _____.

Immediate owner legal name: _____.

(Do not use a "doing business as" name)

Is the immediate owner owned or controlled by another entity: □ Yes or □ No.

(3) If the Offeror indicates "yes" in paragraph (p)(2) of this provision, indicating that the immediate owner is owned or controlled by another entity, then enter the following information:

Highest-level owner CAGE code: _____.

Highest-level owner legal name: _____.

(*Do not use a "doing business as" name*)

(q) *Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law.*

(1) As required by sections 744 and 745 of Division E of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235), and similar provisions, if contained in subsequent appropriations acts, The Government will not enter into a contract with any corporation that–

(i) Has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability, unless an agency has considered suspension or debarment of the corporation and made a determination that suspension or debarment is not necessary to protect the interests of the Government; or

(ii) Was convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless an agency has considered suspension or debarment of the corporation and made a determination that this action is not necessary to protect the interests of the Government.

(2) The Offeror represents that–

(i) It is □ is not □ a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability; and

(ii) It is □ is not □ a corporation that was convicted of a felony criminal violation under a Federal law within the preceding 24 months.

(r) *Predecessor of Offeror.* (Applies in all solicitations that include the provision at 52.204-16, Commercial and Government Entity Code Reporting.)

(1) The Offeror represents that it □ is or □ is not a successor to a predecessor that held a Federal contract or grant within the last three years.

(2) If the Offeror has indicated "is" in paragraph (r)(1) of this provision, enter the following information for all predecessors that held a Federal contract or grant within the last three years (if more than one predecessor, list in reverse chronological order):

Predecessor CAGE code: (or mark "Unknown").

Predecessor legal name:_____.

(*Do not use a "doing business as" name*).

(s) [Reserved].

(t) *Public Disclosure of Greenhouse Gas Emissions and Reduction Goals*. Applies in all solicitations that require offerors to register in SAM (12.301(d)(1)).

(1) This representation shall be completed if the Offeror received $7.5 million or more in contract awards in the prior Federal fiscal year. The representation is optional if the Offeror received less than $7.5 million in Federal contract awards in the prior Federal fiscal year.

(2) Representation. [Offeror to check applicable block(s) in paragraph (t)(2)(i) and (ii)].

(i) The Offeror (itself or through its immediate owner or highest-level owner) □ does, □ does not publicly disclose greenhouse gas emissions, i.e., makes available on a publicly accessible website the results of a greenhouse gas inventory, performed in accordance with an accounting standard with publicly available and consistently applied criteria, such as the Greenhouse Gas Protocol Corporate Standard.

(ii) The Offeror (itself or through its immediate owner or highest-level owner) □ does, □ does not publicly disclose a quantitative greenhouse gas emissions reduction goal, i.e., make available on a publicly accessible website a target to reduce absolute emissions or emissions intensity by a specific quantity or percentage.

(iii) A publicly accessible website includes the Offeror's own website or a recognized, third-party greenhouse gas emissions reporting program.

(3) If the Offeror checked "does" in paragraphs (t)(2)(i) or (t)(2)(ii) of this provision, respectively, the Offeror shall provide the publicly accessible website(s) where greenhouse gas emissions and/or reduction goals are reported:_____.

(u)

(1) In accordance with section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions), Government agencies are not permitted to use appropriated (or otherwise made available) funds for contracts with an entity that requires employees or subcontractors of such entity seeking to report waste, fraud, or abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting such waste, fraud, or abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.

(2) The prohibition in paragraph (u)(1) of this provision does not contravene requirements applicable to Standard Form 312 (Classified Information Nondisclosure Agreement), Form 4414 (Sensitive Compartmented Information Nondisclosure Agreement), or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

(3) *Representation*. By submission of its offer, the Offeror represents that it will not require its employees or subcontractors to sign or comply with internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting waste, fraud, or abuse related to the performance of a Government contract to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information (*e.g.*, agency Office of the Inspector General).

(v) *Covered Telecommunications Equipment or Services-Representation.* Section 889(a)(1)(A) and section 889 (a)(1)(B) of Public Law 115-232.

(1) The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (https://www.sam.gov) for entities excluded from receiving federal awards for "covered telecommunications equipment or services".

(2) The Offeror represents that–

(i) It□ does, □ does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

(ii) After conducting a reasonable inquiry for purposes of this representation, that it □ does, □ does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services.

(End of Provision)

HSAR 3052.209-70 Prohibition on Contracts with Corporate Expatriates (JUN 2006)

(a) Prohibitions.

Section 835 of the Homeland Security Act, 6 U.S.C. 395, prohibits the Department of Homeland Security from entering into any contract with a foreign incorporated entity which is treated as an inverted domestic corporation as defined in this clause, or with any subsidiary of such an entity. The Secretary shall waive the prohibition with respect to any specific contract if the Secretary determines that the waiver is required in the interest of national security.

(b) Definitions. As used in this clause:

Expanded Affiliated Group means an affiliated group as defined in section 1504(a) of the Internal Revenue Code of 1986 (without regard to section 1504(b) of such Code), except that section 1504 of such Code shall be applied by substituting `more than 50 percent' for `at least 80 percent' each place it appears.

Foreign Incorporated Entity means any entity which is, or but for subsection (b) of section 835 of the Homeland Security Act, 6 U.S.C. 395, would be, treated as a foreign corporation for purposes of the Internal Revenue Code of 1986.

Inverted Domestic Corporation. A foreign incorporated entity shall be treated as an inverted domestic corporation if, pursuant to a plan (or a series of related transactions)—

(1) The entity completes the direct or indirect acquisition of substantially all of the properties held directly or indirectly by a domestic corporation or substantially all of the properties constituting a trade or business of a domestic partnership;

(2) After the acquisition at least 80 percent of the stock (by vote or value) of the entity is held—

(i) In the case of an acquisition with respect to a domestic corporation, by former shareholders of the domestic corporation by reason of holding stock in the domestic corporation; or

(ii) In the case of an acquisition with respect to a domestic partnership, by former partners of the domestic partnership by reason of holding a capital or profits interest in the domestic partnership; and

(3) The expanded affiliated group which after the acquisition includes the entity does not have substantial business activities in the foreign country in which or under the law of which the entity is created or organized when compared to the total business activities of such expanded affiliated group.

Person, domestic, and foreign have the meanings given such terms by paragraphs (1), (4), and (5) of section 7701(a) of the Internal Revenue Code of 1986, respectively.

(c) Special rules. The following definitions and special rules shall apply when determining whether a foreign incorporated entity should be treated as an inverted domestic corporation.

(1) *Certain stock disregarded.* For the purpose of treating a foreign incorporated entity as an inverted domestic corporation these shall not be taken into account in determining ownership:

(i) Stock held by members of the expanded affiliated group which includes the foreign incorporated entity; or

(ii) Stock of such entity which is sold in a public offering related to an acquisition described in section 835(b)(1) of the Homeland Security Act, 6 U.S.C. 395(b)(1).

(2) *Plan deemed in certain cases*. If a foreign incorporated entity acquires directly or indirectly substantially all of the properties of a domestic corporation or partnership during the 4-year period beginning on the date which is 2 years before the ownership requirements of subsection (b)(2) are met, such actions shall be treated as pursuant to a plan.

(3) *Certain transfers disregarded*. The transfer of properties or liabilities (including by contribution or distribution) shall be disregarded if such transfers are part of a plan a principal purpose of which is to avoid the purposes of this section.

(d) *Special rule for related partnerships*. For purposes of applying section 835(b) of the Homeland Security Act, 6 U.S.C. 395(b) to the acquisition of a domestic partnership, except as provided in regulations, all domestic partnerships which are under common control (within the meaning of section 482 of the Internal Revenue Code of 1986) shall be treated as a partnership.

(e) Treatment of Certain Rights.

(1) Certain rights shall be treated as stocks to the extent necessary to reflect the present value of all equitable interests incident to the transaction, as follows:

(i) warrants;

(ii) options;

(iii) contracts to acquire stock;

(iv) convertible debt instruments; and

(v) others similar interests.

(2) Rights labeled as stocks shall not be treated as stocks whenever it is deemed appropriate to do so to reflect the present value of the transaction or to disregard transactions whose recognition would defeat the purpose of Section 835.

(f) *Disclosure.* The offeror under this solicitation represents that [Check one]:

__ it is not a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003;

__ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it has submitted a request for waiver pursuant to 3009.108-7004, which has not been denied; or

__ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it plans to submit a request for waiver pursuant to 3009.108-7004.

(g) A copy of the approved waiver, if a waiver has already been granted, or the waiver request, if a waiver has been applied for, shall be attached to the bid or proposal.

(End of provision)

Page 165

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 166

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 167

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Performance Work Statement (PWS)
Department of Homeland Security (DHS),
Immigration and Customs Enforcement (ICE)
Law Enforcement Investigative Database Subscription
October 20, 2020

1. BACKGROUND

The intent of this Performance Work Statement (PWS) is to procure a web-based law enforcement investigative database subscription service to assist Immigration, Customs and Enforcement (ICE) mission of conducting criminal investigations that protect the United States against terrorists and criminal organizations that threaten our safety and national security; to combat transnational criminal enterprises that see to exploit America's legitimate trade, travel and financial systems. ICE investigative agents require a robust analytical research tool for its in-depth exploration of persons of interest and vehicles.

The purpose of this contract is to provide ICE agents an investigative database system to further strategize arrests to minimize and, in some cases, avoid impact of potential injury. ICE requirement of a web-based law enforcement investigative database platform is to include, integration access to public records and commercial data with uninterrupted service, integrate investigative capabilities with the license plate recognition capabilities to be utilized by multiple ICE Directorates to include but not limited to Homeland Security Investigative (HSI), Enforcement and Removal Operations (ERO) and Office of Professional Responsibility (OPR). Use of this database subscription services furthers the criminal law enforcement mission.

1.1 **DHS/ICE**

ICE is the largest investigative agency in the Department of Homeland Security (DHS) and was formally established on March 1, 2003. ICE's primary mission is to protect national security, public safety, and the integrity of the US borders through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration.

ICE investigates a range of domestic and international activities including:

- Human smuggling and trafficking;
- Narcotics, cultural property, weapons and other contraband smuggling;
- Export enforcement, e.g., illegal arms and dual-use equipment;
- Financial crimes;
- Commercial fraud;
- Intellectual property rights violations;
- Cyber-crimes;
- Immigration fraud; and,
- Human rights violations.

The law enforcement investigative database system currently supports over 11,000 users across multiple program areas with analytical data and concrete information to search high risk and politically exposed criminal activity worldwide. The database subscription service plays a

crucial role in ICEs overall investigative mission success. Moreover, the agency can achieve cost savings to the government when reducing the work hours required for physical surveillance.

2.0 SCOPE/OBJECTIVES

The Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement (ICE) houses a large dataset of detailed data that is available to an assortment of approved law enforcement users. ICE criminal law enforcement mission; to enhance investigations to support all mission activities mentioned above in over 50 countries and 67 locations globally; to provide a platform where the continuity of public records and commercial data is available on an uninterrupted basis and to identify criminal suspects, businesses and assets of targets of investigations for potential arrest, seizure and forfeiture will require the usage of a robust investigative database subscription service.

The scope of this requirement is to subscribe to and use the contractor's proprietary data, content and analytical data to optimize ICE operational support functions to enable mission success. This includes supporting all aspects of ICE screening and vetting, lead development, and criminal analysis activities. It also includes, but is not limited to, conducting data extractions to identify unusual trends, data anomalies, and control breakdowns, identifying possible trends, patterns, and links to automate methods for detecting, monitoring, analyzing, summarizing and graphically representing patterns of relationships between entities, identifying potentially criminal and fraudulent behavior before crime and fraud can materialize, and detecting and reporting elements of crimes involving the exploitation or attempts to exploit the immigration and customs laws of the United States.

ICE requires web-based law enforcement investigative databases platform to provide constant (24 hour, seven days per week, 365 days a year) accessibility to a database for ICE law enforcement personnel across the United States in the execution of their official law enforcement duties.

The task areas listed constitute the technical scope of this PWS:

- Task Area 1: Database Functionality Requirements (CLIN 0001)
- Task Area 2: License Plate Reader (LPR) (CLIN 0002)
- Task Area 3: Training and User Management Support (CLIN 0003)

3.0 TASK REQUIREMENTS

The ICE law enforcement investigative database platform shall contain a web-based, centralized database for client management and reporting. Generally, all users shall provide direct input into the database and output requests (reports) shall be generated directly from the database system.

The ICE participating programs shall provide input (i.e., client level data) and the contractor shall provide the database systems administrative and support for report generation. The investigative platform requires the best-supported investigative data and data-analytic management available in the marketplace; to allow readily available access to billions of public records and additional investigative content in an intuitive working environment.

The tasks required under this Performance Work Statement (PWS) require a community-wide data-analytic collection and management system that includes the following:

3.1 TASK AREA 1: DATABASE FUNCTIONAL REQUIREMENTS

- The government's requirement is that the database uses a matching algorithm to return search records that can identify and eliminate duplicated results. The database shall use Entity Resolution applied across results from all sources as they are returned. This maximizes the value of searching multiple sources and saves time by automating the process of record comparison.
- The government's requirement is that the database must be able to interface with FALCON/Raven Palantir systems. The database program shall offer a system-to-system (S2S) connection that merges the database program's public and proprietary data with Palantir analytical information to narrow in and locate persons and assets of interest. (S2S API will replace Palantir connection)
- The government's requirement is that the database must compare the input search criteria and score them against all records in their data sources. The database must use a Relevant Scoring application that allows them to return the most relevant and most current records at the top of the results list.
- The government's requirement is that the database program must have the ability to construct link charts. The database shall use Link-Chart Visualization and Mapping, which allows investigators to save selected results and report data indefinitely and provides the capability to generate link charts and map views of the data.
- The government's requirement is that the database program must allow for multiple searches using unique criteria. Investigators must be allowed to enter specific search criteria once, the system then returns all relevant data, regardless of the source. The program must support search federation against both open-source and internal data repositories and include features like entity resolution, search filtering and charting and mapping across all supported sources.
- The government's requirement is that the database program must allow for Batch Requests where multiple social security numbers (SSN) and or phone numbers may be queried at one time. This capability is both time- and cost-saving for Worksite and Identity Benefit Fraud investigations where multiple SSN's are queried at one time vs. one at a time.
- The government's requirement is that the database must allow for mobile "on the go" access. The law enforcement investigative research tool shall provide full access to core search and report capability from mobile, wireless devices, including HTML5-supported smartphones.
- Available functionality includes person, vehicle, watercraft and phone searches and the National Comprehensive Report. Reports shall be saved automatically in a results tab for future viewing.
- The government's requirement is that the database shall have the ability to conform to the investigator's needs, so reports generated can be customized to an

investigator or analyst case load. Users shall create report templates by setting report preferences, identifying which sections to include, and setting the sequence in which sections are displayed. For example, customers wanting to see only the asset-related information for an individual could create an "Asset Profile" report with the sections they want included, in the order that they want. The law enforcement online research tool shall also offer a workspace feature which allows users to save selected results and report data indefinitely and provides the ability to generate link-chart and map views of the data. Visualizing information on multiple subjects in a link-chart view makes it easier for investigators to discern possible connections or associations between subjects/entities.

- The government's requirement is that the information provided by the law enforcement online research tool should enable ICE to effectively and quickly identify assets currently owned or previously owned/operated by suspect individuals and/or organizations under investigation. The research tool should allow for the flexibility of locating suspects' assets through a multitude of search options. It should also offer the ability to create custom searches so investigators can retrieve information more specific to the time of criminal activity and/or by target name.
- The government's requirement is that the information provided by the law enforcement online research tool should enable ICE OPR to effectively identify searching of a record/document and generate a corresponding audit record. The system shall allow OPR to search sign-on data for the user profile based on a beginning and ending date and time.

- The government's requirement is the system will have the capacity to:
    - Generate program, agency, community, and, if applicable, collaborative level reports.
    - Produce standard, built-in reports and forms to be queried by Area of Responsibility (AOR), to include user reports, agency reports, component, location and sublocation reports and other reports as required.
    - Perform integrated ad hoc reporting that maintains user level security restrictions while allowing for user flexibility in choosing tables and fields as well as filtering and conditional report aspects.
    - Import and export data through XML and CSV formats, imports and exports and ability to securely strip data of identifiers and manage data transmission.
- The government's requirement is that System Security will include Integrated technical safeguards to ensure a high level of privacy and security, including:
    - Back end server(s), including data encryption and transmission
    - Administrator controlled username and password access
    - Automatic timeout/log-off
    - Administrator controlled user level read, write, edit and delete capabilities
    - Administrator controlled user level module and sub-module access
    - Automated audit trail
    - Information Security Industry Standard encryption and SSL certifications

(256-Bit AES encryption)

All technical safeguards required to protect Personally Identifiable Information (PII) All security safeguards required for compliance.

3.2 TASK AREA 2: LICENSE PLATE READER (LPR) REQUIREMENTS

- The LPR data service shall contain LPR records from a variety of sources across the United States, such as toll road or parking lot cameras, vehicles repossession companies and law enforcement agencies.
- The LPR data service shall include substantial unique LPR detection records.
- The LPR data service shall compile LPR from at least 25 states and 24 of the top 30 most populous metropolitan statistical areas to the extend authorized by law in those locations.
    - A metropolitan statistical area is defined as: a geographical region with a relatively high population density at its core and close economic ties throughout the area as defined by the Office of Management and Budget (OMB) and used by the Census Bureau and other federal government agencies for statistical purposes.
- The LPR data service provider shall demonstrate the number of new unique records that were added to the commercially available LPR database each month for the last consecutive twelve (12) months.
- The LPR data service shall make available at least 30 million new unique LPR data records each month.

3.2.1 QUERY CAPABILITIES

- The contract shall ensure that before a user is able to perform a query from the database or mobile application the tool must display upon logon a splash screen that describes the agency's permissible uses of the database application, the data and all user's affirmative consent to the rules of behavior prior to initial entry of the investigative tool.

- The contractor shall ensure the splash screen shall appear at each logon event.
- The contractor shall ensure the text on the splash screen shall also be available to the users via a hyperlink within the main system interface (to include mobile app interface)
- The contractor shall provide the language for the splash screen content.
- All queries of the LPR data service shall be based on a license plate number queried by the user only and the data returned in response must be limited to matches of that license plate number only within the specified period of time.
- The system will not permit user queries of the data service unless a license plate number is entered. A query can only be conducted by entering a license plate number.

- The query interface shall include a drop-down field for users to select a reason code for the query from a pre-populated list. The specific reason codes shall be provided by ICE. This field is mandatory for conducting a query.

- The query interface will require the user to identify whether the user is entering data for either him or herself or for another individual. If the user is entering data for another individual, the query interface will require the user to enter the name of the other individual.

- The query interface must include a free-text field of at least 255 characters for user notes. This will allow for additional information that will assist ICE in referencing the specific case for which the query was performed. Completing this field shall be mandatory for conducting a query.

- The system will have the capability to limit the query by time frame to allow users to comply with agency policy. Depending on the type of investigation being conducted, agency policy will allow the user to query the historical LPR detection records for only a certain period of time (e.g., going back 5 years from the date of query for any immigration investigation).
    - The query interface will have a field for the user to select or input the appropriate timeframe for the query.
    - The system will display results only for LPR detection records within that timeframe (e.g., only for the last 5 years).
    - The system shall not run a query that lacks a time frame entered by the user.

        - The vendor shall guarantee the results of queries meet a high degree of accuracy in datasets, with a margin of error not more than 2%.

        - To ensure accuracy of information, the response to a query must include at least two photos on all hits.
        - Photos must be of sufficient quality to allow the user to visually confirm the license plate and vehicle make/model in the photo are the same as what is represented in the vendor system.

        - Query results must seamlessly integrate with web-based interactive maps. The printable report should show two different map views, nearest address, nearest intersection and coordinates.

        - The vendor shall provide a notification mechanism in the event ICE users identify photographs that do not match the data in their system (license plate numbers or make/model mismatches). The vendor shall address all erroneous data. The vendor shall notify ICE and the ICE user of any inputted erroneous data and keep ICE and ICE users informed of corrections to erroneous data.

- The vendor will not use any information provided by the agency (query data) for its own purposes or share the information with other customers, business partners, or any other entity.

- The vendor will not use ICE's queries (the license plate numbers input into the system) for its commercial purposes. The vendor will only use the queries submitted by ICE to maintain an audit log.

- The vendor will ensure ICE user queries are conducted anonymously to ensure other individuals or entities that use the LPR service (whether a law enforcement agency, commercial entity, or otherwise) are not able to identify that ICE is investigating a license plate.

3.2.2 ALERT LIST CAPABILITIES

- The LPR data service shall provide an "Alert List" feature that will save license plates numbers to query them against new records loaded into the vendor's LPR database on an on-going basis. Any matches will result in a near real-time notification to the user who queried the license plate number.

- The LPR data service Alert List will provide capabilities to share Alert List notifications between ICE users involved in the investigation.

- The Alert List feature will: 1) Automatically match new incoming detection records to user-uploaded or -entered Alert Lists containing the license plate numbers of interest in the investigation; 2) Send an email notification to the user originating such Alert List records and to any ICE user that has been shared the Alert List indicating there is a license plate match to new records in the system; and 3) Provide within the LPR system for download a PDF case file report for the match (with maps, vehicle images, and all pertinent detection & Alert List record information) for each email alert notification. The notification must be able to be limited to the user or a user group of ICE law enforcement officers involved in the specific investigation. The notification will comply with all applicable laws, including the Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725.

- The LPR data service will allow specifically designated users to batch upload a maximum of 2,500 license plate records into the "Alert List". The batch upload will be in the form of a single comma separated variable (CSV) file with data fields to include, but not limited to the following: Plate number; State of Registration; Vehicle Year, Make, Model & Color; reason code and an open text field, of at least 255 characters, for a user note to assist in referencing the specific purpose / investigation / operation for which the query was performed.

- The vendor will provide the ability to establish Alert List submissions, flag license plates for deconfliction, and perform searches, all conducted anonymously, to ensure other individuals or entities that use the LPR service (whether a law enforcement

agency, commercial entity, or otherwise) are not able to identify that ICE is investigating a license plate.

- License plate pictures taken with the automated Optical Character Recognition (OCR) plate number translation shall be submitted to the LPR data service system for matching with license plates on any current ICE Alert List. Any positive matches shall return to the iOS application (identified below) alerting authorized users of a positive match. These pictures will be uploaded into the data service query by an authorized ICE user along with any mandatory information needed for a normal query.

- Each license plate number on an Alert List will be valid for one year unless the user removes it before expiration. If determined to be cost feasible, the system will prompt users two weeks prior to expiration and require the user to affirmatively indicate that there continues to be an operational requirement to keep the particular license plate entry on the Alert List active, or be given the option to delete the license plate from the Alert List. Prompts should continue periodically until the expiration date is reached. The system will grant the user an additional week after expiration to renew the entry in the Alert List. If the user does not renew, the system shall remove the license plate number from the Alert List.

- All Alert List activity shall be audited to capture username, date and time, reason code, and user note associated with the query, as well as license plate number entry, deletion, renewal, and expiration from the alert list.

- The vendor shall not retain any data entered onto an Alert List except as part of the audit trail once the entry has expired per the process described above, or once the user has deleted the entry from the Alert List.

3.2.3 MOBILE DEVICE CAPABILITIES

- The LPR data service shall feature an iOS-compatible mobile application that allows authorized ICE users to:

  - Query the LPR data service by entering the license plate number, state of registration, reason code, and the ability to add returned positive matches into the Alert List.

  - Have quick access and recall of any queries and Alert Lists associated with the user or designated user group. The vendor application will delete any saved data on the mobile device after 60 days, if not already deleted manually by the user.

  - Provide the ability for user to use their mobile device camera to scan full and/or partial license plates to query against various hotlists in the existing IOS compatible application.

- Provide capabilities to share Alert List notifications between ICE users involved in the investigation.

    - The mobile application will conform to all other performance, privacy, and functional requirements identified in the SOW. The vendor shall coordinate with ICE to make sure that the mobile application undergoes the required privacy assessment prior to use.

3.2.4 AUDIT AND REPORTING CAPABILITIES

- The vendor shall generate an immutable audit log in electronic form that chronicles the following data:
    - Identity of the user initiating the query or the person on whose behalf the query is initiated, if different;
    - Exact query entered, to include license plate number, date limitations, geographic limitations (if applicable), reason code, and any other data selected or input by the user;
    - Date and time of query; and
    - Results of the query.

- All Alert List activity shall be audited to capture username, date and time, reason code, and user note associated with the query, as well as license plate number entry, deletion, renewal, and expiration from the alert list.

- The vendor shall provide to ICE user audit reports upon request. Audit reports shall contain the audit log information of a given user(s) for the specified period of time. The vendor shall provide the audit log in electronic form via secure transmission to ICE promptly upon request. The format of the audit log shall allow for ICE to retrieve user activity by username (or ID), query entered (e.g., particular license plate) and date/time. The exact technical requirements and format for the audit log will be negotiated after contract award.

- The vendor shall promptly cooperate with an ICE request to retrieve and provide a copy of the actual records retrieved from the LPR data service in response to a particular query, or any other data relevant to user activity on the vendor system, for purposes of the agency's internal investigations and oversight.

- The vendor shall not use audit trail data for any purpose other than those specified and authorized in this contract.

- The vendor is to provide quarterly and upon request, statistics based on positive hits against the number of requested searches and hit list.

- The audit logs specified in this statement of work are records under the Federal Records Act. The vendor shall maintain these records on behalf of ICE throughout

the life of the contract, but for no more than seven (7) years. The vendor is not authorized to share these records, or the Alert List data, with any outside entities including other law enforcement agencies. At the end of the contract, the vendor shall extract, transfer, and load these records (including any still-active Alert List data, if requested by ICE) to another storage medium or location specified by ICE. This transfer of records shall occur no later than thirty (30) days after the contract ends. After successful transfer of these records, the vendor shall ensure all copies of the records (including any still-active Alert List data) are securely deleted from all networks and storage media under its control or under the control of any of its agents or subcontractors.

- The contractor shall meet the following Key Performance Parameters (KPPs):

Metric	Unit of Measure	Minimum
LPR Data Service	Uptime – Unit of measure 100%	>99.0
	Operating Schedule	24/7/365
	Scheduled downtime	</= 4 hours per month
	Meantime between failure (MTBF)	4,000 operating hours
Overall Support Service	Support availability	24/7/365
Results of LPR Query	Results of a single LPR query	</= 5 seconds after submission

3.3 TASK AREA 3: TRAINING AND USER MANAGEMENT SUPPORT.

The object of this task is to provide training to ICE personnel through on-site, remote, and/or on-demand training on the Law Enforcement Investigative database tool. Training and user management support is implemented to ensure proper guidance and navigation of the database tool is accessible to all assigned users.

- The contract shall provide written instruction manuals and guidance to facilitate use of the database investigative tool and the LPR system.

- The contract shall ensure the user has the ability to compare new user requests with lists of personnel authorized by ICE to utilize the database and LPR tool.

- The contractor shall ensure the all users has automatic verification of accounts with the ability to audit by using the user's Originating Agency Identifier (ORI) to be matched against a current real-time list of active ORI numbers provided directly or indirectly by the National Law Enforcement Telecommunications System (NLETS).

- The contractor shall have the ability to add new users or delete existing users within 24 business hours of ICEs request.

- The contract shall provide initial training or subsequent training to orient persons to the use of the database investigative and LPR tool; to include the "Help Desk" support related to the use, access and maintenance of the tool.

- The contract shall provide system training and escalation procedures as it pertains to agency administrators and shall include procedures for password resets to the database tool.

- The contractor shall provide unlimited technical support for all users.

- The contractor shall perform periodic or as needed updates (maintenance, refresh, etc.) to the overall database tool, web-based interface and mobile application. The contractor shall also ensure to employ appropriate technical, administrative and physical security controls are in place to protect the integrity, availability and confidentiality of the data that resides on all of its systems.

4.0 OTHER APPLICABLE CONDITIONS

4.1 PERIOD OF PERFORMANCE

The Period of Performance will consist of a base year with four (4) one-year options.

4.2 PLACE OF PERFORMANCE

The primary place of performance will be the Contractor's facilities with frequent visits to the, Immigration and Customs Enforcement (ICE) headquarters facilities in the Washington Metro Area.

4.3 TRAVEL

Contractor travel is not required for this requirement. Local meetings or activities planned outside of the defined place of performance are permitted, but all expenses incurred are the responsibility of the contractor.

4.4 POST AWARD CONFERENCE

The Contractor shall attend Post Award Conference with the Contracting Officer and the COR no later than 5 business days after the date of award. The purpose of the Post Award Conference, which will be chaired by the Contracting Officer, is to discuss technical and contracting objectives of this contract. The Post Award Conference will be held either virtually (e.g., MS Teams, Zoom, Adobe Connect, etc.) and/or at the Government's facility, location to be determined via teleconference.

4.5 INVOICES

A standard invoice template shall be provided by the contractor and confirmed by the COR for use on this contract. Invoices shall be verified by the Government COR and submitted on a monthly basis.

4.6 DATA RIGHTS

When applicable; All raw data is to be provided to and shall become the property of the US Government. To include, but not limited to data, deliverables, reports, & solutions in their entirety which are utilized to continually support this contract.

4.7 CONTRACTOR QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

The Contractor shall establish and maintain a Quality Assurance Surveillance Plan (QASP) to ensure the requirements of this contract are provided as specified. The Contractor shall provide a QASP describing the inspection system that they intend to use for the requested services listed. The contractor shall implement procedures to identify, prevent and ensure non-recurrence of defective services. The Contractor's draft QASP shall be required as part of their quote submittal. The CO will notify the Contractor of acceptance or the necessity for QASP modification of the plan no later than 10 business days after award. The Contractor shall provide a final QASP to the COR no later than 20 business days after award. The QASP shall be updated as changes occur and shall be submitted to the COR for review and subsequent CO acceptance by the government. The Performance Requirements Summary (PRS) and Performance Standards Matrix (PSM) is outlined in the Quality Assurance Surveillance Plan (QASP) Appendix A.

5.0 DELIVERABLES

The contractor shall provide the following deliverables in the format and frequency listed.

Deliverables Name	PWS Paragraph	Frequency
Kick-off Meeting/Post Award Conference	4.4	A kick-off meeting with the government will be conducted within 5 days of award. Meeting minutes due from Contractor to COR & CO within 2 business days of the meeting.
Audit report, ad hoc reports, user manuals, etc.	3.2.4 3.3	Reports are due upon request of the COR and/or as required. To include any subsequent updates.
Audit Logs, transfer of records	3.2.4	Provide email confirmation 30 days after contract ends.
Data Rights any work first produced such as user administrative and operations manuals and anything else first produced under this PWS if applicable.	3.2.4	One month prior to the end of the period of performance (POP).

Deliverables Name	PWS Paragraph	Frequency
IT Security Plan	6.4	Within 45 days after contract award.
QASP/Progress Reports	4.7	Draft due to the government proposal. Final QASP due to the COR and CO 20 days after award. Subsequent reports due quarterly and/or as requested.
Invoices	4.5	Invoice should be submitted on a monthly basis to the COR and designated Finance Center for all services performed and no more than 30 days in the arrears of the last day of the POP.

5.1 GENERAL REPORT REQUIREMENTS

The Contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with ICE workstations (Windows XP and Microsoft Office Applications).

5.2 ACCEPTANCE CRITERIA

ICE will accept or reject deliverables within fifteen (15) business days after delivery. If rejected, the Contractor shall make corrections as specified and resubmit the deliverable for review and approval within five (5) business days provided however that contractor is not dependent upon a third party for performance. If the government does not reply within the specific timeframe than the deliverable shall be determined acceptable.

6.0 SECURITY

All solutions and services shall meet DHS Security policy terms and conditions. The Contractor shall ensure that the system(s) complies with DHS/ICE security services and features and Security Sensitive Information controls as detailed in the DHS MD 11042.1 Safeguarding Sensitive but Unclassified (For Official Use Only). In addition, the Contractor shall ensure the system(s) also complies with the following:

6.1 Security Review Terms and Conditions

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford ICE, including the organization of ICE Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer Technical Representative (COTR), and other government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor will contact ICE Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to ICE. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of ICE data or the function of computer system operated on behalf of ICE, and to preserve evidence of computer crime.

6.2 ISA Terms and Conditions

Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be authorized at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements as follows; memoranda of understanding, service level agreements or interconnection security agreements.

6.3 Encryption Compliance Terms and Conditions

If encryption is required, the following methods are acceptable for encrypting sensitive information:

(b)(7)(E)

6.4 Security Requirements for Unclassified Information Technology Resources

The Contractor shall be responsible for IT security for all systems connected to a DHS network or operated by the Contractor for DHS regardless of location. This clause applies to all and any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. Within 45 days after

contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with a further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer (CO), shall be incorporated into the contract as a compliance document. The Contractor's IT Security Plan shall comply with Federal laws that include but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq); the Government Information Security Reform Act of 2000; and the FISMA of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunication systems.
Examples of tasks that require security provisions include:

a) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and
b) Access to DHS networks or computers at a level beyond that granted the public (e.g., such as bypassing a firewall).

At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided the contractor during the contract and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

6.5 Contractor IT Security Accreditation

Within 6 months after contract, the contractor shall submit written proof of IT Security accreditation to DHS for approval by DHS CO. Accreditation will proceed according to the criteria of DHS Sensitive System Policy Publication, 4300A (most current version) or any replacement publication, which the CO will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the CO, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation

6.6 Contractor Employee Access (Sep 2012)

Sensitive Information, as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy.

This definition includes the following categories of information:

a) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland

Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

b) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

c) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

d) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

e) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the CO. Upon the CO's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

The CO may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason. Including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the CO. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

6.7 Safeguarding of Sensitive Information (MAR 2015)

Applicability. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

Definitions. As used in this clause—
"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

> (1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);
>
> (2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and

Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

"Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

a) Authorities. The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information

(2) DHS Sensitive Systems Policy Directive 4300A

(3) DHS 4300A Sensitive Systems Handbook and Attachments

(4) DHS Security Authorization Process Guide

(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information

(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program

(7) DHS Information Security Performance Plan (current fiscal year)

(8) DHS Privacy Incident Handling Guidance

(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html

(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html

(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

b) Handling of Sensitive Information. Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA),*

as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

c) Authority to Operate. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (most current version), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (most current version), or any successor publication, and the *Security Authorization Process Guide* including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) Renewal of ATO. Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) Security Review. The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's

facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) Continuous Monitoring. All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) Revocation of ATO. In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) Federal Reporting Requirements. Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

d) Sensitive Information Incident Reporting Requirements.

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of

discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime contractor location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
(v) Contracting Officer POC (address, telephone, email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected, and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

e) Sensitive Information Incident Response Requirements.

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(i) Inspections,
(ii) Investigations,
(iii) Forensic reviews, and
(iv) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

f) Additional PII and/or SPII Notification Requirements.

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance*. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;
(ii) A description of the types of PII and SPII involved;

(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;

(iv) Steps individuals may take to protect themselves;

(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and

(vi) Information identifying who individuals may contact for additional information.

g) **Credit Monitoring Requirements.** In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;

(ii) Daily customer service;

(iii) Alerts provided to the individual for changes and fraud; and

(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;

(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;

(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;

(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;

(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and

(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

Certification of Sanitization of Government and Government-Activity-Related Files and Information. As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*

6.8 Security Training Requirements

All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually, and the COR will provide notification when a review is required.

6.9 Privacy Training Requirements

All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting*

Personal Information before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

6.10 SECTION 508 COMPLIANCE

Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) as amended by P.L. 105-220 under Title IV (Rehabilitation Act Amendments of 1998) all Electronic and Information Technology (EIT) developed, procured, maintained and/or used under this contract shall be in compliance with the "Electronic and Information Technology Accessibility Standards" set forth by the Architectural and Transportation Barriers Compliance Board (also referred to as the "Access Board") in 36 CFR Part 1194. The complete text of Section 508 Standards can be accessed at http://www.access-board.gov/ or at http://www.section508.gov.

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE OF PAGES
	1 | 4

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. *(If applicable)*
P00002	See Block 16C	192121EROFUGOPS88	

6. ISSUED BY CODE 70CMSD

INVESTIGATIONS & OPS SUPPORT DALLAS
U.S. Immigration and Customs Enforcement
Office of Acquisition Management
8222 N. BELTLINE ROAD, (b)(6); (b)(7)(C)
IRVING TX 75063

7. ADMINISTERED BY *(If other than Item 6)* CODE ICE/IOSD

Investigations Ops Support Dallas
Immigration and Customs Enforcement
Office of Acquisition Management
7701 N. Stemmons Freeway, (b)(6); (b)(7)(C)
Attn: (b)(6); (b)(7)(C) 469) 858-(b)(6); (b)(7)(C)
Dallas TX 75247

Reviewed by LNRS Legal 6.24.21

8. NAME AND ADDRESS OF CONTRACTOR *(No., street, county, State and ZIP Code)*

LEXISNEXIS RISK SOLUTIONS INC
ATTN (b)(6); (b)(7)(C)
1000 ALDERMAN DR
ALPHARETTA GA 300054101

CODE 0601172440000 FACILITY CODE

(x) 9A. AMENDMENT OF SOLICITATION NO.

9B. DATED *(SEE ITEM 11)*

x 10A. MODIFICATION OF CONTRACT/ORDER NO. 70CMSD21C00000001

10B. DATED *(SEE ITEM 13)* 02/25/2021

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended, ☐ is not extended.
Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA *(If required)* Net Increase: $636,536.00
See Schedule

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	
	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: *(Specify authority)* THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES *(such as changes in paying office, appropriation date, etc.)* SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
X	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: FAR 52.212-4 (c) changes
	D. OTHER *(Specify type of modification and authority)*

E. IMPORTANT: Contractor ☐ is not. ☒ is required to sign this document and return 1 copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION *(Organized by UCF section headings, including solicitation/contract subject matter where feasible.)*

DUNS Number: 060117244
Primary COR/Invoicing POC: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Alternate COR/Invoicing POC: (b)(6); (b)(7)(C)
Acquisition POC: (b)(6); (b)(7)(C)

The purpose of this modification is to add Justice Intelligence services to the contract. See attached updated Performance Work Statement (PWS) dated June 17, 2021. This PWS replaces the previous PWS in its entirety. LexisNexis is only responsible for the tasks listed under Tasks 1/1A of the PWS. As a result of the Justice Intelligence addition, the Contract Line Items (CLINs) are changed as follows:

Continued ...

Except as provided herein, all terms and conditions of the document referenced in Item 9 A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER *(Type or print)*		16A. NAME AND TITLE OF CONTRACTING OFFICER *(Type or print)*	
(b)(6); (b)(7)(C) CEO (LNSSI)		(b)(6); (b)(7)(C)	
15B. (b)(6); (b)(7)(C)	15C. DATE SIGNED 06/24/21	16B. UNITED STATES OF AMERICA (b)(6); (b)(7)(C)	16C. DATE SIGNED 6/28/2021

NAME OF OFFEROR OR CONTRACTOR
LEXISNEXIS RISK SOLUTIONS INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	CLIN 0001 is increased by (b)(4) (b)(4) CLIN 1001 is increased by (b)(4) (b)(4) CLIN 2001 is increased by (b)(4) (b)(4) CLIN 3001 is increased by (b)(4) (b)(4) CLIN 4001 is increased by (b)(4) (b)(4) from The total obligated amount on this contract is increased by (b)(4) to (b)(4) The total contract value is increased by (b)(4) to (b)(4) All other terms and conditions remain the same. ~ Period of Performance: 03/01/2021 to 02/28/2022 Change Item 0001 to read as follows(amount shown is the obligated amount):				
0001	LAW ENFORCEMENT INVESTIGATIVE DATABASE SUBSCRIPTION Task 1-Database functionality requirements Task 1A-Training and User Maintenance POP 3/1/21-2/28/22 Justice Intelligence database for up to (b)(4) Enforcement and Removal Officers (ERO) for the remainder of the base period which include 7/1/2021-2/28/2022. Accounting Info: (b)(7)(E) ------ --- Funded: $0.00 Accounting Info: (b)(7)(E) ------ --- Funded: $0.00 Accounting Info: (b)(7)(E) ------ --- Funded: $0.00 Accounting Info: (b)(7)(E) Continued ...				(b)(4)

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	(b)(7)(E) ----- ---				
	Funded: $0.00 Accounting Info: (b)(7)(E) ------ ---				
	Funded: (b)(4)				
	Change Item 1001 to read as follows(amount shown is the obligated amount):				
1001	LAW ENFORCEMENT INVESTIGATIVE DATABASE SUBSCRIPTION Task 1-Database functionality requirements Task 1A-Training and User Maintenance POP 3/1/22-2/28/23 Amount: (b)(4) (Option Line Item) 02/28/2022				0.00
	Change Item 2001 to read as follows(amount shown is the obligated amount):				
2001	LAW ENFORCEMENT INVESTIGATIVE DATABASE SUBSCRIPTION Task 1-Database functionality requirements Task 1A-Training and User Maintenance POP 3/1/23-2/29/24 Amount: (b)(4) (Option Line Item) 02/28/2023				0.00
	Change Item 3001 to read as follows(amount shown is the obligated amount):				
3001	LAW ENFORCEMENT INVESTIGATIVE DATABASE SUBSCRIPTION Task 1-Database functionality requirements Task 1A-Training and User Maintenance POP 3/1/24-2/28/25 Amount: (b)(4) (Option Line Item) 02/29/2024				0.00
	Change Item 4001 to read as follows(amount shown is the obligated amount):				
4001	LAW ENFORCEMENT INVESTIGATIVE DATABASE SUBSCRIPTION Continued ...				0.00

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED 70CMSD21C00000001/PC00C2	PAGE 4 OF 4

NAME OF OFFEROR OR CONTRACTOR
LEXISNEXIS RISK SOLUTIONS INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Task 1-Database functionality requirements Task 1A-Training and User Maintenance POP 3/1/25-2/28/26 Amount: (b)(4) (Option Line Item) 02/28/2025				

Appendix A

Quality Assurance Surveillance Plan (QASP)
License Plate Reader (LPR) Data Service

NOTE: The Government reserves the right to revise or change the QASP as determined by the Government to ensure quality service and deliverables over the course of the contract.

1. PURPOSE

This Quality Assurance Surveillance Plan (QASP) provides a systematic method to evaluate performance for the stated contract. This QASP explains the following:

- What will be monitored
- How monitoring will take place
- Who will conduct the monitoring
- How monitoring efforts and results will be documented

This QASP does not detail how the Contractor accomplishes the work. Rather, the QASP is created with the premise that the Contractor is responsible for management and quality control actions to meet the terms of the contract. It is the Government's responsibility to be objective, fair, and consistent in evaluating performance. In addition, the QASP should recognize that unforeseen and uncontrollable situations may occur.

This QASP is a "living document" and the Government may review and revise it on a regular basis. However, the Government shall coordinate changes with the Contractor. Updates shall ensure that the QASP remains a valid, useful, and enforceable document. Copies of the original QASP and revisions shall be provided to the Contractor and Government officials implementing surveillance activities.

2. GOVERNMENT ROLES AND RESPONSIBILITIES

The following personnel shall oversee and coordinate surveillance activities.

a. Contracting Officer (CO) - The CO shall ensure performance of all necessary actions for effective contracting, ensure compliance with the contract terms, and shall safeguard the interests of the United States in the contractual relationship. The CO shall also ensure that the Contractor receives impartial, fair, and equitable treatment under this contract. The CO is ultimately responsible for the final determination of the adequacy of the Contractor's performance.

b. Contracting Officer's Representative (COR) - The COR is responsible for technical administration of the contract and shall assure proper Government surveillance of the Contractor's performance. The COR shall keep a quality assurance file. At the conclusion of the contract or when requested by the CO, the COR shall provide documentation to the CO. The COR is not empowered to make any contractual commitments or to authorize any contractual changes on the Government's behalf. The Contractor shall refer any changes they deem may affect contract price, terms, or conditions to the CO for action.

c. Other Key Government Personnel - Immigration and Customs Enforcement (ICE) National Fugitive Operations Program Headquarters Staff or Federal employees as designated by the COR and/or CO.

All Point of Contact's (POC) information will be released upon award.

3. PERFORMANCE STANDARDS

Performance standards define desired services. The Contractor is responsible for performance of ALL terms and conditions of the contract. CORs will provide contract progress reports quarterly to the CO reflecting performance on this plan and all other aspects of the resultant contract. The performance

standards outlined in this QASP shall be used to determine the level of Contractor performance in the elements defined.

The Government performs surveillance to determine the level of Contractor performance to these standards. Standards apply to each month of performance.

The Performance Requirements are listed below. The Government will use these standards to determine Contractor performance and shall compare Contractor performance to the standard and assign a rating. At the end of the performance period, these ratings will be used, in part, to establish the past performance of the Contractor on the contract.

The Government will use these standards to determine Contractor performance and compare Contractor performance to the Acceptable Quality Level (AQL).

Table 1: Performance Requirements Summary (PRS)

Metric	Unit of Measure	Minimum AQL
LPR Data Service	Uptime – Unit of measure 100%	> 99.0
	Operating Schedule	24/7/365
	Scheduled downtime	**</= 4 hours per month**
	Meantime between failure (MTBF)	4,000 operating hours
Overall Support Service	Support availability	24/7/365
Results of LPR Query	Result of LPR query after entered in end-user-computing device	</= 5 seconds after submission

Table 2: Performance Standards Matrix

Performance Requirement	Paragraph	Performance Standard	Performance Indicator	Performance Level	Surveillance Method	Government Documentation Criteria
LPR Data Service and Technical Support	3.0 3.1 3.2 3.3	Uptime of Data Service and Technical Support shall be fully available 24/7/365	LEIDS Data Service downtime shall not exceed 4 hours in any 1-month period and Meantime between failure (MTBF) is 4,000 operating hours	> 99.0%	Validated User/Customer Complaints 100% Inspection	Metrics will be reported in CPARS.
Overall Support Service	3.0 3.1 3.2 3.3	Support Availability	Support Service must be available 24/7/365	>99% Monitored monthly during the Transition In period.	Contractor self-monitoring and Validated User/Customer Complaints 100% Inspection	Metrics will be reported in CPARS.
Results of Query	3.2.1 3.2.2 3.2.3	Length of time for Results of LPR query to appear after being entered in the end-user computing device	Less than 5 seconds after submission	95% Monitored monthly during the life of the contract	Contractor Self-monitoring and Validated User/Customer Complaints 100% Inspection	Metrics will be reported in CPARS.

4. METHODS OF QUALITY ASSURANCE (QA) SURVEILLANCE

Regardless of the surveillance method, the COR shall always contact the Contractor's task manager or on-site representative when a defect is identified and inform the manager of the specifics of the problem. The COR, with assistance from the CO, shall be responsible for monitoring the Contractor's performance in meeting a specific performance standard/AQL.

Various methods exist to monitor performance. The COR will use the surveillance methods listed below in the administration of this QASP.

a. PERIODIC INSPECTION

- Scheduled quarterly inspection of audit logs or as required

b. VALIDATED USER/CUSTOMER COMPLAINTS

The Contractor is expected to establish and maintain professional communication between its employees and customers. The primary objective of this communication is customer satisfaction. Customer satisfaction is the most significant external indicator of the success and effectiveness of all services provided and can be measured through customer complaints.

Performance management drives the Contractor to be customer focused through initially and internally addressing customer complaints and investigating the issues and/or problems, but the customer always has the option of communicating complaints to the COR, as opposed to the Contractor.

Customer complaints, to be considered valid, must be set forth clearly and in writing the detailed nature of the complaint, must be signed, and must be forwarded to the COR.

Customer feedback may also be obtained either from the results of customer satisfaction surveys or from random customer complaints.

- Review of identified deficiencies and or complaints made by users of the services
- Investigate and validate
- Review of notification of report discrepancies

c. 100% INSPECTION

- Review of LPR Data Service uptime
- Review of Scheduled Downtime
- Review Meantime Between Failure (MTBF)
- Review Overall Support Service Availability

d. Analysis of Contractor's progress report. The Contractor is required to provide a weekly progress report that will be used to communicate the Contractor's status in the Transition phase.

e. Performance reporting.

Surveillance results will be used as the basis for actions against the Contractor Past Performance Report. In such cases, the Inspection of Services clause in the Contract becomes the basis for the CO's actions.

5. DOCUMENTING PERFORMANCE

Documentation must be accurate and thorough. Completeness, currency, and accuracy support both satisfactory and unsatisfactory performance

a. ACCEPTABLE PERFORMANCE

The Government shall document positive performance. All positive performance should be documented by an email to the COR describing the outstanding performance and why it is of value to the Government. This information shall become a part of the supporting documentation for the Contractor Performance Assessment Reporting System (CPARS) and the QASP

b. UNACCEPTABLE PERFORMANCE

When unacceptable performance occurs, the COR shall inform the Contractor. This will be in writing unless circumstances necessitate verbal communication. In any case the COR shall document the discussion and place it in the COR file.

When the COR determines formal written communication is required, the COR shall prepare a Contract Discrepancy Report (CDR) and present it to the Contractor's representative. A CDR template is available upon request to the Contracting Officer.

The Contractor will acknowledge receipt of the CDR in writing. The CDR will specify if the Contractor is required to prepare a corrective action plan to document how the Contractor shall correct the unacceptable performance and avoid a recurrence. The CDR will also state how long after receipt the Contractor has to present this corrective action plan to the COR. The Government shall review the Contractor's corrective action plan to determine acceptability.

Any CDRs will become a part of the supporting documentation for Past Performance.

6. FREQUENCY OF MEASUREMENT

While the Contractor is fully expected to comply with all requirements in the PWS, the Government’s assessment of Contractor performance will focus mainly on the objectives listed in the AQL column of the Performance Standards Summary Matrix. The COR will monitor the Contractor’s performance to ensure it meets the standards of the contract. Unacceptable performance may result in the Contracting Officer taking any of the following actions: Require the Contractor to take necessary action to ensure that future performance conforms to contract requirements, reduce the contract price to reflect the reduced value of the services, issue a Contract Discrepancy Report, or require the Contractor to re-perform the service. In addition, the Contractor’s performance will be recorded annually in the Contractor Performance Assessment Report (CPAR).

From: (b)(6); (b)(7)(C)
To:
Cc:
Subject: RE: LEIDS Funding Allocation Info
Date: Thursday, February 11, 2021 3:51:31 PM
Attachments: image001.jpg

Yes, it was. Thank you (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)
Management and Program Analyst
Acquisition Management Unit
Finance, Acquisition, Asset Management Division
Homeland Security Investigations (HSI)
202-573 (Mobile)
(b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)

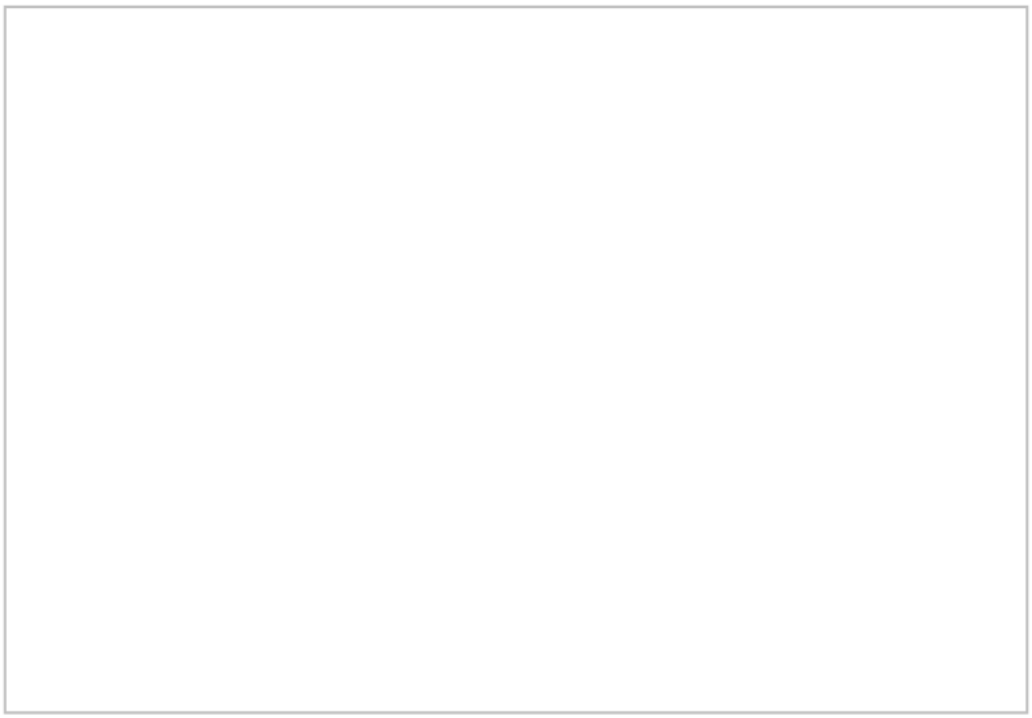
From: (b)(6); (b)(7)(C)
Sent: Thursday, February 11, 2021 3:51 PM
To (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: LEIDS Funding Allocation Info

That was a quick update. Thanks (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Thursday, February 11, 2021 3:50 PM
To: (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: LEIDS Funding Allocation Info

It was reallocated yesterday.

(b)(6); (b)(7)(C); (b)(7)(E)



(b)(6); (b)(7)(C)
Office of Professional Responsibility
U.S. Immigration & Customs Enforcement

iPhone: (202) 270(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Thursday, February 11, 2021 3:48 PM
To: (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: LEIDS Funding Allocation Info

Hi (b)(6);

I sent a request to have the funds moved. However we are no longer capable of moving funds in-house. The request has to go through OBPP. I will follow up and get back to you soon with a status update.

Thank you,
(b)(6);
(b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Thursday, February 11, 2021 3:43 PM
To: (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: LEIDS Funding Allocation Info

Hi (b)(6); (b)(7)(C)

Reaching back to see if you had an opportunity to move the funding to the org code (b)(7)(E)
(b)(7)(E) (while retaining the same project-task, fund, program & object class codes). It appears HSI has received

funding. Thanks for your help.

R,

(b)(6);
(b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Management and Program Analyst
Acquisition Management Unit
Finance, Acquisition, Asset Management Division
Homeland Security Investigations (HSI)
202-573- (Mobile)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Wednesday, February 3, 2021 5:41 PM
To: (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: LEIDS Funding Allocation Info

Hi (b)(6); (b)(7)(C)

No problem. I'll work on it tomorrow.

Thank you!
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Wednesday, February 3, 2021 5:31 PM
To: (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: LEIDS Funding Allocation Info

Hi (b)(6); (b)(7)(C)

Thanks for the gentle reminder. I have received a response from HSI Finance with regards to the funding strings. Is it possible to move the funding to the org code (b)(7)(E) while retaining the same project-task, fund, program & object class codes)? This will make an easier transition during the fund & approve process of the requisition. Also, we are still waiting for ICE to fund Q2.

(b)(6); (b)(7)(C)
(b)(6);
(b)(7)(C)
Management and Program Analyst
Acquisition Management Unit
Finance, Acquisition, Asset Management Division
Homeland Security Investigations (HSI)
202-573- (Mobile)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Wednesday, February 3, 2021 4:09 PM
To: (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)

Subject: RE: LEIDS Funding Allocation Info

Good afternoon (b)(6); (b)(7)(C)

The funding for the contract is still on our line. Is there something additional HSI needs from us?

Thank you,

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) | **Management and Program Analyst**
U.S. Department of Homeland Security
Office of Professional Responsibility | Operational Support Unit
Mobile: (703) 867 (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Monday, February 1, 2021 1:15 PM
To: (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: LEIDS Funding Allocation Info

Hi (b)(6); (b)(7)(C)

I would proceed with the funding allocation that you provided. The conversation with management agreed upon the (b)(4) I will revisit the final IGCE. Thanks for the update.

(b)(6); (b)(7)(C)
Management and Program Analyst
Acquisition Management Unit
Finance, Acquisition, Asset Management Division
Homeland Security Investigations (HSI)
202-573- (Mobile)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Monday, February 1, 2021 12:31 PM
To: (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: LEIDS Funding Allocation Info

Hi (b)(6); (b)(7)(C)

This is the last pricing we received and budgeted for (option B). Is this still the case?

Investigative Tool Description	(b)(4); (b)(7)(E)
Tool Standard Features	
Administrative Portal	
Search Functions	
LPR	

Total	(b)(4)

From: (b)(6); (b)(7)(C)
Sent: Monday, February 1, 2021 12:18 PM
To: (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: LEIDS Funding Allocation Info

Hi (b)(6); (b)(7)(C)

Thank you for the update. I have forwarded an itemized break out to our Finance folks (see below). I think we're ok at the moment; however, please note that the funds are to be received no later than next week. I will prepare the G514 upon receipt of your funds. Thank you.

IGCE for the base year of this contract is the following:

	Description	Total Cost Est	HSI	ERO	OPR
BY	Database Subscription + LPR	(b)(4)			
BY	Database Subscription				
BY	LPR				

(b)(6); (b)(7)(C)
Management and Program Analyst
Acquisition Management Unit
Finance, Acquisition, Asset Management Division
Homeland Security Investigations (HSI)
202-573 (Mobile)
(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Monday, February 1, 2021 12:07 PM
To: (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: LEIDS Funding Allocation Info

Hi (b)(6); (b)(7)(C)

Unfortunately I haven't had anyone get back to me. Do you think HSI will give us an extension? I can reach out to the HSI POC directly if you would like.

Thank you,
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Monday, February 1, 2021 9:41 AM
To: (b)(6); (b)(7)(C) />
Cc: (b)(6); (b)(7)(C)
Subject: RE: LEIDS Funding Allocation Info

Ok, roger that. Thanks so much!

(b)(6); (b)(7)(C)
Management and Program Analyst
Acquisition Management Unit
Finance, Acquisition, Asset Management Division
Homeland Security Investigations (HSI)
202-57 (Mobile)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Monday, February 1, 2021 9:39 AM
To: (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: LEIDS Funding Allocation Info

Hi

I am working with our budget team now and will get back to you shortly.

Thank you,
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Monday, February 1, 2021 8:14 AM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: LEIDS Funding Allocation Info

Good Morning (b)(6); (b)(7)(C)

I hope your weekend was an enjoyable one. As promised I am reaching out to begin the funding process of LEIDS. May I please request the funding allocation for the OPR support. It just so happens that HSI Finance is requiring the funding strings for LEIDS and will need this info **no later than Noon** today. I appreciate your assistance and if you can provide this information at your earliest. Let me know if you have any questions. Thank you.

(b)(6); (b)(7)(C)
Management and Program Analyst
Acquisition Management Unit
Finance, Acquisition, Asset Management Division
Homeland Security Investigations (HSI)
202-573 (Mobile)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Tuesday, January 26, 2021 10:55 AM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: LEIDS RFP Posted Dec 7

Good morning (b)(6); (b)(7)(C)

All is great, thanks for asking. I hope all is well with you.

Fantastic! We anticipate prepping the G514 to fully fund this effort soon. The TET wrap up of Phase II (User Trial period) comes to a close next week. Then OAQ will begin the award decision process (multiple upper management reviews). Currently on target to award Feb 16. I shall keep you posted. Thanks again for the update.

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

Management and Program Analyst
Acquisition Management Unit
Finance, Acquisition, Asset Management Division
Homeland Security Investigations (HSI)
202-573 (Mobile)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Tuesday, January 26, 2021 10:45 AM
To: (b)(6); (b)(7)(C)
Subject: RE: LEIDS RFP Posted Dec 7

Good morning (b)(6); (b)(7)(C)

I hope all is well. Good news. OPR has the funds to proceed. Please keep me updated on the status and let me know what you need from me as we go.

Thank you!
(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) **Management and Program Analyst**
U.S. Department of Homeland Security
Office of Professional Responsibility | Operational Support Unit
Mobile: (703) 867 (b)(6); (b)(7)(C)

From (b)(6); (b)(7)(C)
Sent: Tuesday, January 5, 2021 2:06 PM
To (b)(6); (b)(7)(C)
Subject: RE: LEIDS RFP Posted Dec 7

(b)(6); (b)(7)(C) no worries, I understand. I'll standby until I hear back from you. Thanks so much!

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

Management and Program Analyst
Acquisition Management Unit
Finance, Acquisition, Asset Management Division
Homeland Security Investigations (HSI)
202-573 (Mobile)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)

Sent: Tuesday, January 5, 2021 2:01 PM
To: (b)(6); (b)(7)(C)
Subject: RE: LEIDS RFP Posted Dec 7

Happy New Year too!

OPR is going over funds now, I'll find out if we have the funds and get back to you. I really appreciate it.

Thanks!
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Tuesday, January 5, 2021 1:54 PM
To: (b)(6); (b)(7)(C)
Subject: RE: LEIDS RFP Posted Dec 7

Good afternoon (b)(6); (b)(7)(C)

Happy New Year! The LEIDS contract is scheduled for an award date of no later than March 1. However, the CO is targeting a February 16 (if all goes well) award. My hope is to have the funds obligated within the first week of February. Let me know if that will work for OPR.

Also, I received an email today from HSI management advising that funds have not been received nor the apportionment and as soon as this info becomes available they will be in touch. I hope this helps. Let me know if I can further assist.

(b)(6); (b)(7)(C)
Management and Program Analyst
Acquisition Management Unit
Finance, Acquisition, Asset Management Division
Homeland Security Investigations (HSI)
202-573 (Mobile)
(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Tuesday, January 5, 2021 1:23 PM
To: (b)(6); (b)(7)(C)
Subject: RE: LEIDS RFP Posted Dec 7

Good afternoon (b)(6); (b)(7)(C)

Do you happen to know when the funds for this contract need to be obligated?

Thank you,
(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) **| Management and Program Analyst**
U.S. Department of Homeland Security
Office of Professional Responsibility | Operational Support Unit
Mobile: (703) 867 (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Monday, December 7, 2020 4:02 PM
To: (b)(6); (b)(7)(C) ;
(b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C) >
Subject: LEIDS RFP Posted Dec 7

Good Afternoon All,

I hope everyone is doing well. News flash the Law Enforcement Investigative Database Subscription (LEIDS) solicitation is now posted. I've attached the solicitation, government answers to industry questions and other applicable docs for your situational awareness. The aggressive schedule is set forth as follows:

Acquisition Event	Estimated Completion Date
Release of RFQ	December 7, 2020
Question & Answers	December 9, 2020
Phase 1-Oral Presentations	December 14-18, 2020
Evaluation of Phase I	December 14-18, 2020
Phase II-User Trial Period	January 4-22, 2021
Award Decision Approvals	February 5, 2021
Congressional Notification	February 5, 2021
Award Date	February 15, 2021

I shall keep you abreast of any updates. Thank you all for your continued support and patience.

(b)(6); (b)(7)(C)
Management and Program Analyst
Acquisition Management Unit
Finance, Acquisition, Asset Management Division
Homeland Security Investigations (HSI)
202-573 (Mobile)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Monday, December 7, 2020 12:02 PM
To: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Subject: FW: Government responses to industry December 7, 2020

Forgot to include you ladies…

V/r,
(b)(6); (b)(7)(C)
Investigations & Operations Support Dallas | Contracting Officer

DHS | ICE | Office of Acquisition Management (OAQ)
Phone 214-905-(b)(6); (b)(7)(C)
Mobile 469-858-
E-mail (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Monday, December 07, 2020 11:00 AM
To: (b)(6); (b)(7)(C)
Subject: Government responses to industry December 7, 2020

See attached Government responses to industry on the Draft solicitation. The final solicitation will be released later today.

V/r,

(b)(6); (b)(7)(C)
Investigations & Operations Support Dallas | Contracting Officer
DHS | ICE | Office of Acquisition Management (OAQ)
Phone 214-905-(b)(6); (b)(7)(C)
Mobile 469-858-
E-mail (b)(6); (b)(7)(C)