Privacy Impact Assessment
for the

Department of Homeland Security State, Local, and Regional Fusion Center Initiative

December 11, 2008

Contact Point
Robert Riegle
Director
State and Local Program Managers Office
Intelligence and Analysis
Department of Homeland Security
(703) 235-0760

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Executive Summary

This Privacy Impact Assessment is required under Section 511 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (the Act), and is conducted by the DHS Chief Privacy Officer under the Authority of Section 222 of the Homeland Security Act of 2002, as amended. This Privacy Impact Assessment (PIA) examines the privacy implications of the State, Local and Regional Fusion Center Initiative, as well as for DHS' State and Local Program Management Office (SLPMO) which has managerial responsibility for the SLFC Program.

The Act codified a number of activities the Department, through the SLPMO, was already undertaking with fusion centers around the country to facilitate information flow in two directions. This includes the placement of a number of DHS senior intelligence analysts within State and local fusion centers. These analysts are in place in order to further the mission of the Department of Homeland Security, and more specifically, the statutory role of the Intelligence and Analysis Directorate found in Title II of the Homeland Security Act.

The Act contains a number of provisions specifically addressing privacy. This includes a requirement to conduct this PIA. Additionally, analysts must complete privacy training developed by the Chief Privacy Officer, and the Secretary of Homeland Security must issue guidelines to ensure State and local participants receive appropriate privacy training. These guidelines must also ensure that fusion centers craft written privacy policies, consistent with Federal and State law.

Finally, the Act places the Initiative within the scope of the Information Sharing Environment (ISE) whenever terrorism, homeland security, and law enforcement information related to terrorism, is shared. Accordingly, the participants in the Initiative must follow all the guidance issued by the President or Program Manager of the ISE (PM-ISE) including those relating to the protection of personal privacy. Through its Privacy Guidelines Committee (PGC), the PM-ISE has issued guidance and other resources to ensure the fusion centers establish privacy policies which are "at least as comprehensive" as the requirements applicable to Federal agencies under the ISE Privacy Guidelines. At this time, the fusion centers have initiated the process to comply with these requirements, and the DHS Privacy Office will monitor their progress.

Even before passage of the 9/11 Act, the Department took a number of steps to embed privacy into the management of the fusion center program and encouraged the fusion centers to consider privacy in their practices. These included:

1. Disseminating the Fusion Center Guidelines developed by the Global Justice Information Sharing Initiative. The Privacy Office encourages fusion centers to implement the guidelines and use the tools provided with them. In particular, Guideline 8 recommends a number of elements fusion centers should include in

their privacy policies: Add introductory language that clearly states the privacy practices of the center; Describe the information collected and how the information is stored; Establish a common lexicon of terms for dealing with role-based access; Define and publish how the information will be used; Draft a clear, prominent, and understandable policy; Display the privacy policy for both center personnel and customers; Ensure that all other policies and internal controls are consistent with the privacy policy; Establish a business practice of notifying government agencies of suspected inaccurate data; Adhere to applicable state and federal constitutional and statutory civil rights provisions; Partner with training centers on privacy protection requirements and conduct periodic privacy security audits; Consult with the privacy committee (established pursuant to Guideline 3) to ensure that citizens' privacy and civil rights are protected; When utilizing commercially available databases, ensure that usage is for official business and the information is not commingled with private sector data. To prevent public records disclosure, risk and vulnerability assessments should not be stored with publicly available data; and, Determine if there are security breach notification laws within the jurisdiction and follow those laws, if applicable.

2. Participating in the Information Sharing Environment. The DHS Privacy Office is a member of the Privacy Guideline Committee, and a member of the Privacy Office staff co-chairs the PGC's State, local, and Tribal Government working group. This working group is specifically tasked with establishing guidance to assist fusion centers with establishing privacy policies at least as comprehensive as Federal members of the ISE.

3. Public Outreach. The Privacy Office has participated in a number of efforts to enhance public understanding of the fusion center program. On September 18, 2007, the Privacy Office held a public meeting of its Data Privacy and Integrity Advisory Committee focusing on fusion centers. Committee members and the attending public heard testimony from Federal, State and local participants, as well as from members of the privacy advocacy community. The Privacy Office has also attended meetings between the SLPMO and representatives of advocacy groups, where concerns about privacy were discussed.

4. Training. The Privacy Office made presentations to both the Southern Shield Conference and the Southeast Regional Fusion Center conference, introducing the Global Fusion Center Guidelines and the ISE Privacy Guidelines, and has toured a number of individual fusion centers around the country.

   In addition, the Privacy Office is fulfilling its training responsibilities under the Act. To date, all DHS intelligence analysts assigned to a fusion center have received at least two hours of specialized training conducted by the Privacy Office, and each analyst

assigned in the future will receive the same training before assuming the post. Moreover, the Office is teaming with other Federal partners to develop training suitable for State and local fusion center representatives.

5. Information Sharing Fellows Program and the Interagency Threat Assessment Coordination Group. The 9/11 Commission Act created two more programs which will interact with fusion centers: the Information Sharing Fellows (ISF) program and the Interagency Threat Assessment Coordination Group (ITACG). Each is the subject of its own PIA fully describing the privacy issues raised by the programs. As these initiatives mature, we anticipate that they will become a strong influence in the amount and character of information making its way to State and local participants in the fusion center Initiative. For this reason, and consistent with the statutory requirement in the 9/11 Commission Act, participants in both programs will receive privacy training. The Privacy Office expects that this training will provide an additional layer of privacy sensitivity into the fusion center Initiative.

Section 222 of the *Homeland Security Act* of 2002, states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the *Privacy Act of 1974*. In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. They are: Transparency; Individual Participation; Purpose Specification; Data Minimization; Use Limitation; Data Quality and Integrity; Security; and Accountability and Auditing. This PIA examines the methods the SLPMO employs to implement the FIPPs, and points to guidance issued by the PM-ISE which calls on individual fusion centers to implement each FIPP in their own policies.

Despite these efforts, the Privacy Office has identified a number of risks to privacy presented by the fusion center program:

1. Justification for fusion centers
2. Ambiguous Lines of Authority, Rules, and Oversight
3. Participation of the Military and the Private Sector
4. Data Mining
5. Excessive Secrecy
6. Inaccurate or Incomplete Information
7. Mission Creep

This PIA examines these issues and explains the mitigation strategies for those risks, giving life to the FIPPs. Where necessary, the Privacy Office offers recommendations on how DHS (and

individual fusion centers) can take additional action to further enhance the privacy interests of the citizens they are charged with protecting.

This PIA is neither the beginning nor the end of the Privacy Office's engagement with the fusion center Initiative. Looking forward, the Privacy Office will continue to provide training to DHS personnel assigned to fusion centers, to State and local fusion center representatives, as well as to participants in the ISF and ITACG programs. In addition, the Privacy Office will continue to examine the program and monitor progress of program participants, and report our findings in an updated PIA.

The Privacy Office regularly reviews and revises PIAs as we learn more information about a program or how program changes impact individual privacy. Moreover, Congress explicitly mandated that the Privacy Office issue a report on the privacy impact of the program one year after the passage of the 9/11 Commission Act. The Privacy Office anticipates that the training it is developing for fusion centers and the promulgation of guidance from the PM-ISE will contribute to further increasing privacy protections in the Initiative. The next Privacy Office report on the fusion center Initiative will focus on these developments, as well as examine the steps the participants have taken to mitigate the privacy risks identified above. No doubt additional risks will be identified. The Privacy Office is committed to working with Initiative participants to continuously monitor and enhance the privacy protections in place, giving the fullest expression to the FIPPs.

Table of Contents

Abstract

Pursuant to Section 511 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (the "9/11 Commission Act" or "the Act"), Public Law No. 110-53, the Department of Homeland Security (DHS) Privacy Office is conducting a Privacy Impact Assessment (PIA) on the Homeland Security State, Local, and Regional Fusion Center Initiative (the Initiative).[1] Under the Initiative, DHS will facilitate appropriate, bi-directional information sharing between the Department and State, Local, and Regional Fusion Centers. In addition, the Department will assign trained intelligence analysts to fusion centers, provided those centers meet a number of criteria set forth in the text. The Act requires the Department to complete a concept of operations (CONOPS) for the Initiative, including a PIA. The CONOPS also includes a Civil Liberties Impact Assessment, conducted by the DHS Office for Civil Rights and Civil Liberties.

Introduction

This PIA examines the privacy implications of the State, Local and Regional Fusion Center Initiative, established by the 9/11 Commission Act, as well as for DHS' State and Local Program Management Office (SLPMO) which has managerial responsibility for the SLFC Program, and which predates the Act. It begins with a discussion of the specific authority for the Initiative provided within the Act. Then, since the Department's interactions with fusion centers and the SLPMO existed before the Act passed, the PIA includes a background section, examining the underpinnings of the fusion center concept. Next, the PIA catalogs ongoing efforts to infuse privacy into the program including dissemination of fusion center guidelines respecting individual privacy; support for the Information Sharing Environment (ISE); participation in public outreach; providing privacy training to participants in the Initiative; and steps to imbed privacy into programs which are expected to interact with the fusion center Initiative. The PIA then examines how the program's existing policies and procedures implement the Fair Information Practice Principles (FIPPs). Finally, the PIA examines specific privacy concerns raised by the creation and operation of the Initiative and steps participants have taken to mitigate those concerns. Wherever possible, the PIA includes recommendations the Department and individual fusion centers may take in order to further reduce their impact on the privacy of the American Public.

At the outset, it is important to note six particulars about State and local fusion centers and the SLPMO which impact the scope of this PIA. First, as noted, State and local fusion centers existed before Congress established the Initiative. And DHS was already engaged with fusion centers around the country through the creation of a State and Local Management Program before passage of the Act. This ongoing participation also includes awarding grants supporting the

[1] Traditionally, the Privacy Office conducts PIAs under Section 208 of the E-Government Act of 2002 (Pub. Law 107-347) (44 U.S.C. § 101) or under its inherent authority to do so in Section 222 of the Homeland Security Act of 2002 (Pub. Law 107-110) (6 U.S.C. §142).

development and operation of various fusion centers, assigning senior intelligence analysts from DHS' Office of Intelligence and Analysis (I&A) to fusion centers around the country,[2] and facilitating the two-way flow of information in support of the Department's homeland security missions. While one of the primary goals of the Initiative is to increase information sharing, it does not contemplate new avenues of communication. Therefore, the existing privacy compliance documentation—SORNs and PIAs relating, principally, to the Homeland Security Operations Center (HSOC),[3] Operations Directorate Homeland Security Information Network Database,[4] Homeland Security Information Network Communities of Interest,[5] and the Treasury Enforcement Communication System[6]—is sufficient to cover the increased flows of information. Of course, those documents, like this one, are updated whenever necessary.

Second, as their names imply, State and local fusion centers are run by organs of State, local, and tribal governments, and not the Federal Government. No two fusion centers define or carry out their missions in exactly the same way or are subject to the same authorities or regulations. Notions of comity and federalism, moreover, prohibit the Department from placing certain requirements on fusion centers.

Despite the variety of state laws governing each fusion center, all are familiar with the requirements of 28 CFR Part 23, Criminal Intelligence Systems Operating Policies, which includes privacy requirements for Federally funded criminal intelligence systems at use in the States. In discussions with a number of fusion centers, the Privacy Office found that they typically apply the protections developed for their covered criminal intelligence systems for all of their systems. Part 23, moreover, served as the foundation for many of the recommendations related to privacy found within the Global Justice Information Sharing Initiative (Global)'s Fusion Center Guidelines (Global Guidelines). In turn, Global's Guideline 8, relating to privacy, served as a significant inspiration for the Program Manager for the ISE's (PM-ISE) development of its fusion center guidance. Therefore, familiarity and compliance with 28 CFR Part 23 will serve the fusion centers well as they adopt recommendations of the ISE, and is, as a result, discussed in this PIA.

A third, and related, point is that many fusion centers have an "all crimes and/or all-hazards" mission, which is substantially broader than the homeland security mission the Initiative supports. Fusion centers may grapple with any number of issues of exclusively local concern, often with no Federal information or other support. In these cases, their processes and procedures—including those to protect privacy—are their own. The Privacy Office presumes that the States are interested in preserving and competent to protect the rights of their own citizens, and offers no opinion as to their methods.

---

[2] There are currently 25 senior I&A analysts assigned to 23 fusion centers.
[3] HSOC is now called the National Operations Center (NOC). The SORN was published April 18, 2005, 70 FR 20061 and the PIA is published at www.dhs.gov/privacy.
[4] The PIA is published at www.dhs.gov/privacy.
[5] The General Information Technology Access Accounts Records (GITAARs) SORN covers this collection and was last published 73 FR 28139. The PIA is available at www.dhs.gov/privacy.
[6] The SORN was published on October 18, 2001 and can be found at 66 FR 52984.

Fourth, the DHS is not the only Federal agency interacting with fusion centers. Fusion centers receive funding and other assistance from the Department of Justice (DOJ). FBI Agents are assigned to numerous fusion centers and share information with them in both directions under their own arrangements.

Fifth, not all information shared between the Department and fusion centers contains personally identifiable information (PII). A great deal of information is more general, and does not raise any privacy concerns. Even when raw data contains PII before it is shared, Federal participants must delete PII if the recipient is not authorized to receive it or does not need to know it. State and local participants should do so as well. The Privacy Office believes that this type of review can reduce the amount of PII to the bare minimum necessary to share in order to secure the homeland.

Finally, and most importantly, fusion centers and the DHS program to support them are still relatively new. Federal efforts to provide policy guidance to fusion centers are underway. Currently, for instance, the PM-ISE is still developing the material which will specifically address privacy protections required of fusion centers participating in the ISE. In addition, content is still being created for the privacy training requirements established under the 9/11 Commission Act for State and local fusion center representatives. For this reason, this PIA focuses on the current efforts of the DHS to engage with fusion centers, in cooperation with a number of other Federal partners, to infuse privacy into fusion center operations. As the ISE disseminates it policies and the fusion centers implement their policies in response, the privacy protections in fusion centers will become more mature and demonstrable. Thus, when future versions of this PIA are written, the Privacy Office anticipates moving beyond the privacy goals presented herein, to a more traditional assessment of how the fusion centers are meeting their responsibilities to protect privacy as members of the ISE.

These six facts help define the proper scope for this PIA, which is limited to the privacy implications of the DHS State, Local and Fusion Center Initiative's use of PII. This will necessarily include discussion of some issues predating the passage of the 9/11 Commission Act, which created the Initiative. It will reach some actions the States are taking, as well. However, the Privacy Office acknowledges that this PIA will not cover all of the conceivable privacy issues raised by either the involvement of DOJ or all the practices of the States who manage and operate various fusion centers. These are best addressed by the individual States themselves, and the Privacy Office encourages them to do so in a manner akin to this PIA.

This PIA will be updated to reflect changes in the Federal, State, Regional, and Local Fusion Center Initiative over time, particularly as guidance from the PM-ISE is disseminated and implemented. In addition, DHS will issue a report to Congress on the privacy and civil liberties impact of the program, not later than one year after the program is implemented.

Authority: Codification in the 9/11 Commission Act

In August 2007, the President signed the 9/11 Commission Act, which, among many

things, amended the Homeland Security Act to include a Section 210A, relating to the establishment of the State, Local and Regional Fusion Center Initiative, within I&A at DHS, codifying many of the interactions the Department was already undertaking with fusion centers.

Specifically, the Act directs that the Secretary, in consultation with the PM-ISE, the Attorney General, the Chief Privacy Officer of the Department, the Officer for Civil Rights and Civil Liberties of the Department, and the Privacy and Civil Liberties Oversight Board (PCLOB),[7] is tasked with establishing the Department of Homeland Security State, Local, and Regional Fusion Center Initiative.

The purpose of the Initiative is to improve information sharing, in two directions, between State, local and regional fusion centers and the Department of Homeland Security. Fusion centers are defined in the Act as, "a collaborative effort of 2 or more Federal, State, local, or tribal government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity." In fulfilling this mission, the Department shall:

(1) provide operational and intelligence advice and assistance to State, local, and regional fusion centers;

(2) support efforts to include State, local, and regional fusion centers into efforts to establish an information sharing environment (ISE);

(3) conduct tabletop and live training exercises to regularly assess the capability of individual and regional networks of State, local, and regional fusion centers to integrate the efforts of such networks with the efforts of the Department;

(4) coordinate with other relevant Federal entities engaged in homeland security-related activities;

(5) provide analytic and reporting advice and assistance to State, local, and regional fusion centers;

(6) review information within the scope of the ISE, including homeland security information, terrorism information, and weapons of mass destruction information, that is gathered by State, local, and regional fusion centers, and to incorporate such information, as appropriate, into the Department's own such information;

(7) provide management assistance to State, local and regional fusion centers;

(8) serve as a point of contact to ensure the dissemination of information within the scope of the ISE, including homeland security information, terrorism information, and weapons of mass destruction information;

(9) facilitate close communication and coordination between State, local, and regional fusion centers and the Department;

[7] The PCLOB is currently administratively inactive.

(10) provide State, local, and regional fusion centers with expertise on Department resources and operations;

(11) provide training to State, local, and regional fusion centers and encourage such fusion centers to participate in terrorism threat-related exercises conducted by the Department; and

(12) carry out such other duties as the Secretary determines are appropriate.

The Act provides that I&A shall assign officers and intelligence analysts to fusion centers, to the extent possible. In order to qualify for such an assignment, candidates must come from certain Departmental components and have relevant work experience. Moreover, analysts must complete training consistent with 28 CFR Part 23, as well as receive "appropriate privacy and civil liberties training that is developed, supported, or sponsored by the Privacy Officer… and the Officer for Civil Rights and Civil Liberties of the Department."[8]

DHS officers or intelligence analysts assigned to fusion centers are responsible for:

(1) assisting law enforcement agencies and other emergency response providers of State, local, and tribal governments and fusion center personnel in using information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, to develop a comprehensive and accurate threat picture;

(2) reviewing homeland security-relevant information from law enforcement agencies and other emergency response providers of State, local, and tribal governments;

(3) creating intelligence and other information products derived from such information and other homeland security-relevant information provided by the Department; and

(4) assisting in the dissemination of such products, as coordinated by the Under Secretary for Intelligence and Analysis, to law enforcement agencies and other emergency response providers of State, local, and tribal governments, other fusion centers, and appropriate Federal agencies.

To ensure the DHS analysts carry out their duties, the Act provides that the analysts assigned to fusion centers have appropriate access to all relevant Federal databases and information systems, consistent with any policies, guidelines, procedures, instructions, or standards established by the President or, as appropriate, the PM-ISE for the implementation and management of that environment.

The Act contains a number of provisions specifically addressing privacy, in addition to the training requirements for analysts mentioned above. For instance, the Secretary is required to issue guidelines ensuring that fusion centers provide non-Federal participants with "appropriate

[8] Section 511(a) of the Act.

privacy and civil liberties training." These guidelines must further ensure that fusion centers "develop, publish, and adhere to a privacy and civil liberties policy consistent with Federal, State, and local laws," and ensure that "appropriate security measures are in place for the facility, data, and personnel."

Finally, the Act expressly places the Initiative within the scope of the ISE[9] whenever terrorism, homeland security, or law enforcement information related to terrorism, is shared.[10] Accordingly, the participants in the Initiative must follow all the guidance issued by the President or PM-ISE relating to the sharing of terrorism, homeland security, and law enforcement information related to terrorism, including those relating to the protection of personal privacy.

---

[9] The ISE is discussed in more detail below. For a comprehensive description of the background and authorities for the ISE, please see the ISE website: http://www.ise.gov/pages/background.html. (May 1, 2008)

[10] The following definitions may be found on the ISE website: http://www.ise.gov/pages/scope.html (May 1, 2008):

Terrorism Information is defined by Section 1016(a)(5), Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, as amended:

- The existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;
- Threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;
- Communications of or by such groups or individuals;
- Groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and
- Includes weapons of mass destruction information. "The term *weapons of mass destruction information* means information that could reasonably be expected to assist in the development, proliferation, or use of a weapon of mass destruction (including a chemical, biological, radiological, or nuclear weapon) that could be used by a terrorist or a terrorist organization against the United states, including information about the location of any stockpile of nuclear materials that could be exploited for use in such a weapon that could be used by a terrorist or a terrorist organization against the United States." Section 1016(a)(6), IRTPA.

Homeland Security Information is defined in Section 892(f) of the Homeland Security Act of 2002. It means any information possessed by a Federal, state, local, or tribal agency that relates to (A) a threat of terrorist activity; (B) the ability to prevent, interdict, or disrupt terrorist activity; (C) the identification or investigation of a suspected terrorist or terrorist organization or any person, group, or entity associated with or assisting a suspected terrorist or terrorist organization; or (D) a planned or actual response to a terrorist act.

Law Enforcement Information - For purposes of the ISE, the term means any information obtained by or of interest to a law enforcement agency or official that is both (A) related to terrorism or the security of our homeland and (B) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of, or response to, criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

Background

Because DHS' cooperation with fusion centers existed before enactment of the 9/11 Commission Act, a brief review of the philosophical underpinnings for the fusion concept and particular events leading up to the creation of the Department's State and Local Fusion Centers Program Management Office (SLFC PMO) is instructive.

Law Enforcement Intelligence and Intelligence-Led Policing

At the heart of fusion centers lies law enforcement intelligence, a concept that is distinct from "intelligence" as most Americans think of the term, national security intelligence. Understanding the distinction is important.

Information is the key to intelligence, of whatever kind. Information has been defined as "pieces of raw, unanalyzed data that identifies persons, evidence, events, or illustrates processes that indicate the incidence of a criminal event or witnesses or evidence of a criminal event." In the law enforcement or criminal context, information includes criminal histories and driving records; statements by witnesses, informants, and suspects; vehicle registration information; banking and other financial information; and police reports.

Law enforcement intelligence and criminal intelligence are used synonymously. Different organizations have defined the terms differently, however. The International Association of Chiefs of Police (IACP) defines criminal intelligence as "[i]nformation compiled, analyzed and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity." The Department of Justice defines criminal intelligence information as:

(3) data which has been evaluated to determine that it:

(i) Is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and

(ii) Meets criminal intelligence system submission criteria.

The Bureau of Justice Affairs within the Department of Justice has stated that "information plus analysis equals intelligence."

As the definitions make clear, intelligence is an analytic process. To render the information gathered useful, it must be analyzed. Analysis is the "derivation of meaning from data." Analysis can be tactical or operational, or it can be strategic, and the resulting intelligence can be tactical or strategic. Tactical intelligence allows law enforcement to solve a particular crime, while strategic intelligence provides the "big picture."

Distinct from criminal intelligence, national security intelligence is the collection and analysis of information concerning the United States, its relationship with foreign governments and non-state actors, regarding political and economic factors, and the maintenance of sovereign US principles. National security intelligence is focused more on the security of the Nation and

the conduct of foreign affairs. It is not focused on the prosecution and conviction of individuals. The risk in the use of national security intelligence is that it may not be amenable to use in a criminal proceeding, rendering its use questionable as direct evidence in a criminal prosecution. Second, the sources and methods used to gather the information that is the basis of the national security intelligence may be compromised if used in a criminal proceeding.

In the mid-nineties, law enforcement officials across the Nation (and indeed, the world) understood a need to incorporate more intelligence analysis, primarily criminal intelligence, into the conduct of their duties. The movement became known as "Intelligence Led Policing" (ILP). The International Association of Law Enforcement Intelligence Analysts (IALEIA) defined Intelligence Led Policing as "the collection and analysis of information to produce an intelligence end product designed to inform police decision-making at both the tactical and strategic level." With this starting point, IALEIA identified three common, fully integrated, elements of an ILP model:

1. The production of accurate and timely intelligence and analytic products, relevant to the operational goals of the agency that describe the nature and extent of problems affecting the jurisdiction.
2. The use of these intelligence and analytical products to develop and guide a strategy, operational plan or course of action that addresses the problems.
3. The continuing evaluation, follow-up and accountability to determine the impact of the strategy or operational plan on the problems, making adjustments as necessary.

Because of the perceived need, what eventually became the fusion center model arose well before passage of the 9/11 Act, and in some cases before the terrorist attacks against the Nation on September 11, 2001.[11]

Law Enforcement Intelligence Sharing, Leading to Global Guidelines and Creation of Fusion Center Program

Not long after 9/11, IACP assembled law enforcement experts from across the country and from Europe to talk about information sharing. At the March 2002 IACP Criminal Intelligence Sharing Summit, the participants recognized that non-Federal agencies must be "more than adjuncts to a national strategy for improved intelligence collection, but founding partners of any organization." Further, the sharing of information and intelligence should extend beyond terrorism, to include all criminal intelligence.

The Summit called for a national intelligence plan, bringing together Federal and non-Federal law enforcement agencies "and their partners in emergency response" to share relevant intelligence. Key to the plan would be the Criminal Intelligence Coordinating Council (CICC) to

[11] See International Association of Law Enforcement Intelligence Analysts, Inc., 1997. *Intelligence Led Policing: International Perspectives on Policing in the 21st Century.* Lawrenceville, IALEIA.

oversee and implement the plan. The Summit made some significant recommendations for the CICC. First, it should ensure that "relevant data" flows to all entities that need the data. Second, there must be a "broad-based effort for improving criminal intelligence generation and sharing." Third, the Federal Government cannot lead exclusively in improving intelligence sharing. Fourth, law enforcement officers are not the only responders with a role in public safety.

The work at the Summit received Federal attention. Global, a Federal advisory committee to DOJ and the Attorney General, provided support to the Summit. In response to the Summit, Global put together the Global Intelligence Working Group (GIWG), which drafted the National Criminal Intelligence Sharing Plan (NCISP), the national intelligence plan envisioned by the Summit. State, local and tribal governments were involved in its drafting. Building on the work of the IACP summit, the plan made 28 recommendations. Highlights of the recommendations focus on law enforcement agencies at all levels working together to strengthen homeland security and foster intelligence-led policing; establishing the CICC; using 28 CFR Part 23 and the Law Enforcement Intelligence Unit Criminal Intelligence File Guidelines; protecting privacy and civil liberties by using, to the extent possible the *Justice Information Privacy Guideline: Developing, Drafting and Assessing Privacy Policy for Justice Information Systems*; and identifying and working on an architecture for sharing information among Federal, State, local, and tribal governments. The Attorney General adopted the NCISP.

With the NCISP as a blueprint, by 2004 many States commenced establishing information fusion centers with various local, State, and Federal funds, to serve as the lynchpin of their intelligence-led policing initiatives, and as the eventual point of exchange for intelligence and information sharing between Federal Government and State, local and tribal governments. At the time, however, no standards or guidelines existed to assist with interoperability and communication issues between the information sharing partners. As a result, centers designed to share information were actually silos of information, incapable of information exchange.

In response, DOJ—at the request of the CICC—formed the Law Enforcement Intelligence Fusion Center Focus Group (FCFG). Concurrently, the DHS Homeland Security Advisory Council (HSAC) Intelligence and Information Sharing Working Group focused its attention on prevention and information sharing by developing guidelines for local and State agencies in relation to the collection, analysis, and dissemination of terrorism-related intelligence (i.e. the fusion process). The recommendations resulting from DOJ's initiative and HSAC's efforts laid the foundation for the development of the Fusion Center Guidelines for law enforcement—and eventually the expansion of those guidelines to include public safety personnel and the private sector.

Secretary of Homeland Security Michael Chertoff signed and endorsed the DHS State and Local Fusion Center Support Implementation Plan as Departmental policy in June 2006. The Implementation Plan first emphasized that State and local governments are among DHS' primary partners, and that State and Local Fusion Centers (SLFC) represent the coherent point of exchange for intelligence and information to be passed between Federal Government and State, local and tribal governments.

The Implementation Plan directed the creation and deployment of integrated DHS teams to SLFCs—to include both operational and intelligence personnel. The Implementation Plan designates I&A—and more specifically—the Chief Intelligence Officer [CINT] as the Executive Agent for Departmental interaction with SLFC. To continue to strengthen and sustain the Department's relationships with SLFCs the Implementation Plan formally established a State and Local Fusion Center Program, and assigned the day-to-day management of the program to a SLPMO. The responsibility to "enable the National Fusion Center Network" by deploying personnel and information systems and "strengthen their ability to add value to the national knowledge base" is tasked to the SLPMO as steward of the SLFC Program. Under this authority, the Department began deploying analysts to fusion centers around the Nation.

Thus, when the 9/11 Commission Act was signed, it codified activities that were substantially underway, including those to protect privacy.

DHS Privacy Office Interaction with Fusion Centers

Even before passage of the 9/11 Act, then, the Department took a number of steps to embed privacy into the management of the fusion center program and encouraged the fusion centers to consider privacy in their practices. This includes disseminating the Global Guidelines, participation in the foundation of the ISE, as well as direct contact with fusion centers, and exploring the privacy issues at a public meeting of the Data Privacy and Integrity Advisory Committee (DPIAC).

Global Justice Information Sharing Initiative Guidelines

The fullest example of DHS' participation was the creation and dissemination of the "Fusion Center Guidelines: Developing and Sharing Information in a New Era," (Global Guidelines) issued in August 2006 by Global, DHS, and DOJ.[12]

Privacy concerns and methods of addressing them appear throughout the Global Guidelines. Global Guideline 3, for instance, urges the inclusion of a privacy committee in the fusion center governance structure. The purpose of this privacy committee will be to "liaise with community privacy advocacy groups to ensure civil rights and privacy protection." Fusion center governing bodies, moreover, are encouraged in this Guideline to collaborate with DHS, including the Privacy Office, to establish their operating processes.

Global Guideline 5 urges fusion center partners to utilize memoranda of understanding (MOUs) to govern interactions between the participants and commit the parties to the principles and policies of the fusion center. The guideline advises that adherence to privacy and security principles should be specifically addressed within all such MOUs.

[12] The Global Guidelines are available online at http://it.ojp.gov/documents/fusion_center_guidelines.pdf (accessed September 13, 2008).

Global Guideline 8 is dedicated to promoting meaningful and lawful privacy policies at the fusion centers, and to providing mechanisms ensuring that the centers adhere to these policies. This begins with consideration of the Fair Information Practice Principles (FIPPs), which are the worldwide baseline for privacy protection—consideration of which is also, appropriately, required by the ISE privacy guidelines. The Fusion Center Guidelines provide a useful list of complementary elements for the drafters of the privacy policy, including:

- Add introductory language that clearly states the privacy practices of the center;
- Describe the information collected and how the information is stored;
- Establish a common lexicon of terms for dealing with role-based access;
- Define and publish how the information will be used;
- Draft a clear, prominent, and understandable policy;
- Display the privacy policy for both center personnel and customers;
- Ensure that all other policies and internal controls are consistent with the privacy policy;
- Establish a business practice of notifying government agencies of suspected inaccurate data;
- Adhere to applicable state and federal constitutional and statutory civil rights provisions;
- Partner with training centers on privacy protection requirements and conduct periodic privacy security audits;
- Consult with the privacy committee (established pursuant to Guideline 3) to ensure that citizens' privacy and civil rights are protected;
- When utilizing commercially available databases, ensure that usage is for official business and the information is not commingled with private sector data. To prevent public records disclosure, risk and vulnerability assessments should not be stored with publicly available data; and
- Determine if there are security breach notification laws within the jurisdiction and follow those laws, if applicable.

Having defined the key elements of a sound privacy policy, the rest of Guideline 8 focuses on the measures the leaders of each fusion center should take to ensure the policy is followed. These steps include such prudent steps as ensuring adequate training and information privacy awareness and establishing a policy for tracking and reviewing privacy complaints and concerns.

Global Guideline 9 provides a framework for ensuring adequate security measures are in place. This includes security for facilities, data, and personnel. Following these security recommendations will ultimately serve privacy by protecting data from unauthorized access.

The supplemental materials available on the Guidelines' companion CD are particularly useful. They include DOJ's Privacy and Civil Rights Policy Templates for Justice Information Systems, Privacy Policy Templates, and a Privacy Policy Development Guide.

The Privacy Office encourages fusion centers to continue their efforts to implement the recommendations of the Global Guidelines and utilize the tools they offer as a substantial step to ensuring individual privacy is protected as the information flows contemplated by the Initiative grow.

The Information Sharing Environment

DHS also supports the ISE, which is active in promoting privacy within fusion centers. The ISE was mandated in December 2004 with the enactment of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).[13] On December 16, 2005, the President issued a Memorandum to the Heads of Executive Departments and Agencies on the Guidelines and Requirements in Support of the Information Sharing Environment, which specified tasks, deadlines, and assignments necessary to further the ISE's development and implementation. The Memorandum directed that the ISE leverage ongoing information sharing efforts in the development of the ISE. The assignments included five guidelines, as follows:

1. Define common standards for how information is acquired, accessed, shared, and used within the ISE;
2. Develop a common framework for the sharing of information between and among executive departments and agencies and state, local, and tribal governments, law enforcement agencies, and the private sector;
3. Standardize procedures for sensitive but unclassified information;
4. Facilitate information sharing between executive departments and agencies and foreign partners; and
5. Protect the information privacy and other legal rights of Americans.

This fifth guideline mandated the creation of ISE Privacy Guidelines, which requires all ISE agencies to take specific and uniform actions that reflect basic privacy protections and best practices, including:

- Identify and review protected information that may be shared in the ISE;
- Enable ISE participants to determine the nature of the protected information that may be shared and any applicable legal restrictions;
- Share protected information in the ISE only to the extent it is terrorism related information;
- Assess, document, and comply with applicable laws and policies;
- Establish data accuracy, quality, and retention procedures;

[13] Public Law 108-458.

- Deploy adequate security measures to safeguard protected information;
- Implement adequate accountability, enforcement, and audit mechanisms to verify compliance;
- Establish redress procedures;
- Implement ISE Privacy Guidelines requirements via changes to business processes and systems, training, and technology;
- Make the public aware of agency policies, as appropriate;
- Ensure that nonfederal entities, including State, local and tribal governments, can access ISE information only if they have privacy policies at least as comprehensive as the ISE Privacy Guidelines;
- Designate a senior official to be accountable for implementation of the Guidelines (ISE Privacy Official); and
- Develop and implement a written ISE privacy protection policy that sets forth the agency's mechanisms, policies, and procedures for implementation of the Guidelines.

Further, the PM-ISE established an ISE Privacy Guidelines Committee (PGC), of which the DHS Chief Privacy Officer is a member. This committee works in collaboration with the PCLOB as well as State, local, and tribal representatives to develop further guidance on the implementation of the Guidelines. The DHS Privacy Office further supports this effort as it relates to fusion centers by co-chairing the State, local, and tribal Government working group of the PGC.

While the initial focus of the PGC has been to provide guidance to Federal agencies, such as the recent issuance of the *Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment*, this work will form the basis for establishing the minimum requirements that State, local, and tribal agencies must meet in establishing privacy policies that are "at least as comprehensive" as the requirements applicable to Federal agencies under the ISE Privacy Guidelines.

Fusion centers represent a valuable information resource and are expected, as they achieve a baseline capability, to play an increasingly important role in terrorism-related information sharing between Federal agencies and State, local, and tribal governments, becoming the focal, though not exclusive, points within each State for the receipt and sharing of terrorism related information. This may include such tasks as validating requests for information from State, local, and tribal offices prior to submission to the Federal Government and ensuring timeliness of information dissemination and sharing by understanding and defining State, local, and tribal information and intelligence requirements.

The Presidential Guideline 2 Report on the common framework for information sharing recommends that fusion centers, in concert with State, local, and tribal entities, undertake the following critical activities and responsibilities in coordination with their Federal partners:

1. Share information to address national security and criminal investigations in a manner that protects privacy, civil liberties, and other legal rights of individuals protected by United States law, while ensuring the security of the information shared;
2. Foster a culture of fusing "all crimes with national security implications" with "all hazards" information in order to capture criminal activity that may be a precursor to a terrorist plot;
3. Support efforts to detect and prevent terrorist attacks by maintaining situational awareness of threats, alerts, and warnings;
4. Develop critical infrastructure protection plans to ensure the security and resiliency of infrastructure operations;
5. Prioritize emergency management, response, and recovery planning activities based on likely threat scenarios and at-risk targets;
6. Determine the allocation of funding, capabilities, and other resources; and
7. Develop training, awareness, and exercise programs.

In addition to receiving, publishing, and disseminating Federal agency information to their State, local, and tribal counterparts, it is essential that fusion centers ensure that locally-generated terrorism information, including Suspicious Activity Reports (SAR) information, be communicated consistent with applicable Federal law to the Federal Government in the ISE. Such terrorism information will, in turn, be disseminated as appropriate to other Federal, State, local, tribal, private sector, and foreign partner entities.

In cooperation with the PM-ISE, the DHS Privacy Office has begun to introduce the ISE requirements to fusion center representatives. A member of the DHS Privacy Office attended the Southwest Regional Fusion Center Conference, hosted by DOJ's Bureau of Justice Assistance (BJA), in Savannah, Georgia on November 6, 2007. Following the presentation of his paper entitled, *The Importance of Privacy in the Information Sharing Environment*, the Privacy Office representative helped introduce the draft *Fusion Center Privacy Policy Development: Privacy and Civil Rights, and Civil Liberties Policy Template*. The Privacy Office recognizes that the creation of a clear written privacy policy is a critical first step in ensuring privacy is protected within the fusion center program. In addition to this meeting with dozens of fusion center attendees, the DHS Privacy Office has toured and discussed privacy protections in fusion centers in Jacksonville and Tallahassee, Florida; Atlanta, Georgia; Baltimore, Maryland; Las Vegas, Nevada; and Centennial, Colorado.

Other Public Outreach

On September 18, 2007, the Privacy Office held a public meeting of the DPIAC dedicated almost entirely to the subject of fusion centers and privacy. The committee heard testimony from the DHS Under Secretary for Intelligence and Analysis, as well as the Civil Liberties Protection Officer of the Office of the Director of National Intelligence, who co-chairs the ISE PWC. In addition to these officials, there was testimony from a panel including the Director of I&A's State

and Local Program Office; the Watch Commander at the Maryland Coordination and Analysis Center (MCAC), a fusion center in Baltimore, Maryland; and a representative from the PM-ISE.

The privacy advocacy community participated as well. The committee heard from representatives of the Electronic Privacy Information Center (EPIC), The Constitution Project, and The American Civil Liberties Union (ACLU).

The Privacy Office also participated in a meeting between the I&A State and Local Program Office, the DHS Office for Civil Rights and Civil Liberties, the MCAC, the Constitution Project, and the ACLU. In addition to this meeting, the Privacy Office is aware that a number of fusion centers throughout the Nation have hosted meetings with representatives of their local privacy advocacy communities.

The Privacy Office is committed to enhancing transparency in DHS programs. Public meetings like the September DPIAC meeting, and private information exchanges like the one hosted at I&A (and at fusion centers around the country) will assist the public in understanding the mission and practices of the Initiative. To the extent possible, the Department and other Initiative participants should continue to take affirmative actions like these to increase interaction, understanding, and transparency within their communities.

Training

The Privacy Office has initiated its training responsibilities under the 9/11 Commission Act. In February 2008, the Privacy Office, the DHS Office for Civil Rights and Civil Liberties, and I&A signed a Memorandum of Agreement to collaborate on training for the Initiative. First, the offices focused on I&A analysts currently assigned to a fusion center. All of these individuals received the CD, *Culture of Privacy Awareness*, and were expected to review it prior to the two one-hour training webinars, conducted by members of the DHS Privacy Office.[14] The initial session was held in April, 2008; privacy topics included the FIPPs and Privacy Act compliance. A second session took place in June, 2008, covering standards for handling PII and requirements following data breaches. The Privacy Office and the Office for Civil Rights and Civil Liberties will continue refining this material and present it to all field officers from DHS in advance of their placement in fusion centers. In addition to fulfilling this statutory requirement, the Privacy Office believes these well-trained DHS officials will become privacy "ambassadors" to the fusion centers where they serve, and their State and local colleagues will witness the fine examples they set.

The Privacy Office and the Office for Civil Rights and Civil Liberties will also work together on training for State and local representatives in fusion centers. For this effort, DHS is partnering with DOJ BJA as well as the PM-ISE. For the privacy portions of the training, the Privacy Office anticipates creating a set of tools for fusion centers which will introduce these participants to Federal privacy law and policy; the PIA process; the FIPPs; the requirements of the

[14] The Privacy Office and Office for Civil Rights and Civil Liberties conducted these sessions together. Participants, then, received a total of four hours of training (in addition to the introductory materials) focusing on privacy, civil rights and civil liberties.

ISE; and other topics identified during a needs assessment phase of development. Finally, the training sessions will stress the importance of State and local employees understanding their own jurisdictions' privacy protection framework.

Information Sharing Fellows Program and the Interagency Threat Assessment Coordination Group

The 9/11 Commission Act created two more programs that will interact with fusion centers: the Information Sharing Fellows (ISF) program and the Interagency Threat Assessment Coordination Group (ITACG). Each is the subject of its own PIA fully describing the programs, so the descriptions here are brief.

Under the ISF, State, local and tribal Law Enforcement Officers (LEOs) and intelligence analysts will be detailed to the Department to participate in the work of I&A in order to become familiar with both the relevant missions and capabilities of the Department and other Federal agencies, and the role, programs, products, and personnel of I&A. In addition, the program is designed to promote information sharing between the Department and State, local, and tribal LEOs and intelligence analysts by assigning such DHS officers and analysts to:

(1) serve as a point of contact in the Department to assist in the representation of State, local, and tribal information requirements;

(2) identify information within the scope of the ISE that is of interest to State, local, and tribal LEOs, intelligence analysts, and other emergency response providers;

(3) assist Department analysts in preparing and disseminating products derived from information within the scope of the ISE that are tailored to State, local, and tribal LEOs and intelligence analysts, and designed to prepare for and thwart acts of terrorism; and

(4) assist Department analysts in preparing products derived from information within the scope of the ISE that are tailored to State, local, and tribal emergency response providers, and assist in the dissemination of such products through appropriate Department channels.

The ITACG is comprised of State, local, and tribal homeland security and law enforcement officers and intelligence analysts detailed and assigned to work at the National Counterterrorism Center with Federal intelligence analysts for the purpose of integrating, analyzing, and assisting in the dissemination of Federally-coordinated information within the scope of the ISE.

As the ISF and ITACG mature, we can anticipate that they will become a strong influence in the amount and character of information making its way to State and local participants in the fusion center Initiative. For this reason, and consistent with the statutory requirement in the 9/11 Commission Act, participants in both programs will receive privacy (and civil liberties) training. The Privacy Office expects that this training will provide an additional layer of privacy sensitivity into the fusion center Initiative.

Fair Information Practice Principles

The Privacy Act of 1974 articulates concepts of how the Federal Government should treat individuals and their information and imposes duties upon Federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002, Section 222(a)(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

In response to this obligation, the DHS Privacy Office developed a set of FIPPs from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. These principles first appeared in the Health Education and Welfare Report, which was the basis for passage of the Privacy Act. The FIPPs account for the nature and purpose of the information being collected, maintained, used, and disseminated in relation to DHS' mission to preserve, protect, and secure. They are: Transparency; Individual Participation; Purpose Specification; Data Minimization; Use Limitation; Data Quality and Integrity; Security; and Accountability and Auditing.

DHS conducts PIAs on both programs and information technology systems, pursuant to the E-Government Act of 2002 Section 208 and the Homeland Security Act of 2002 Section 222. Given that the Initiative is a program rather than a particular information technology system, this PIA is explores how the Initiative implements the FIPPs.

1. Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a system of record notice (SORN) and PIA, as appropriate. There should be no system the existence of which is a secret to the general public.

The Initiative is not intended to change the way information is gathered, collected, used, maintained, or disseminated by DHS. The vast majority of information exchanges by and among the DHS and the fusion centers take place via well established channels, which are the subject of prior privacy compliance documentation. For instance, the Department and many States communicate with each other utilizing the Homeland Security Information Network (HSIN). HSIN is divided into a number of Communities of Interest (COIs), including the Law Enforcement COI, the COI where most information exchanges take place by and between DHS and fusion centers.[15] On June 22, 2007, DHS published a PIA on the HSIN COIs, which establishes the criteria for HSIN COIs. For the Law Enforcement COI, for instance, applicants must demonstrate to DHS that they have a legitimate law enforcement need for access to the COI. This step will help ensure that only law enforcement personnel will have the ability to access any PII that is communicated through this HSIN COI.

[15] The Emergency Management COI is also commonly used, but the instance of PII shared via this COI is rare.

Information is generally sent to and received from fusion centers by the Department's National Operations Center (NOC)[16] within the DHS Operations Coordination and Planning Directorate. The establishment of the Initiative will not change this. Clearly, an important goal of the Initiative is to increase the flow of information in both directions, but it is not intended to create new channels for information exchange or new Federal systems. The database created to store information with a relevant nexus to terrorism at the NOC, which may be either received from or shared with a State, is the subject of a PIA entitled "Homeland Security Information Network Database," published by the Department on April 5, 2006. This too is available on the Privacy Office website. A corresponding SORN entitled "Homeland Security Operations Center" was published in the Federal Register on April 18, 2005 (70 FR 20156). The PIA outlines the information sharing between DHS and other Federal, state, county, local, tribal, private-sector commercial, and other non-governmental organizations involved in identifying and preventing terrorism as well as in undertaking incident management activities.

In addition to this formal documentation, the Department continues to promote transparency through the means discussed in the introduction to this PIA, including public meetings of the DPIAC and information exchanges with the privacy advocacy community. In addition, the public has ample opportunity to learn more about the Initiative through reading Congressional testimony by DHS officials, including the Chief Privacy Officer, and public reports issued by the Government Accountability Office and the Congressional Research Service.[17] The Privacy Office, moreover, encourages the individual fusion centers to make their own privacy documentation, including their written privacy policies and PIAs, available to the public, and to implement Global's Fusion Center Guideline Three, creating a privacy committee to liaise with their local privacy advocacy communities.

As with any intelligence or criminal law enforcement effort, providing the right amount of transparency is key to success. If there is too much transparency, the program will be ineffective because criminals and terrorists will use the information to skirt the law and avoid detection. On the other hand, too little transparency and the public will not trust the program. In order to mitigate the risk of individuals not knowing about the program, as noted above, DHS has existing SORNs and/or PIAs for the systems that I&A analysts have access to, and has reviewed those documents to ensure that I&A's uses of PII are consistent with those documents. Again, this compliance documentation relates principally to the Homeland Security Operations Center (HSOC now NOC), the Operations[18] Directorate Homeland Security Information Network (HSIN) Database, the Homeland Security Information Network Communities of Interest, and the Treasury

[16] The NOC was formerly known as the Homeland Security Operations Center.
[17] See, e.g. ., Prepared Statement of the DHS Chief Privacy Officer Before the House Homeland Security Committee on March 14, 2007; Congressional Research Service, *Fusion Centers: Issues and Options for Congress*. Washington, 2007, CRS; United States Government Accountability Office, GAO-08-35, *Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers*. Washington, 2007, GAO
[18] The Operations Directorate is now the Operations Coordination and Planning Directorate.

Enforcement Communication System. Each is available on the DHS Privacy Office's public website: www.dhs.gov/privacy, and each is updated as necessary.

2. Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS' use of PII.

It should be noted that individual participation is not always possible within criminal and intelligence systems; information in SARs, law enforcement bulletins, and information supplied by other Initiative participants will not always be sourced to the individual they relate to, a point raised in the HSIN database PIA. Nonetheless, the Global Guidelines state that information should be collected with the knowledge or consent of the data subject, where appropriate and possible.

Additionally, both the Global Guidelines and the ISE Privacy Guidelines make recommendations for establishing a redress policy. Again, in intelligence and law enforcement settings, full and open redress is not always possible, as giving subjects access to information stored about them may alert them to an ongoing investigation. The HSIN Database PIA describes a process where individuals can submit "First-Party Amplifying Information," which will be entered into the system if it relates to a record in the system. However, no information about the records in the system will be shared with the subject. Fusion centers are encouraged to establish similar procedures to track and handle privacy complaints and concerns. Where fuller redress mechanisms are possible, they should be implemented.

3. Purpose Specification

Principle: DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purposes for which the PII is intended to be used.

DHS and fusion center participants are expected to seek or retain information that is legally permissible under applicable laws, regulations, policies and Executive Orders. For I&A, this begins with its statutory mission defined under Title II of the Homeland Security Act:

- to access, receive, and analyze law enforcement information, intelligence information, and other information from… State and local government agencies (including law enforcement agencies), and private sector entities, and to integrate such information in order to—(A) identify and assess the nature and scope of terrorist threats to the homeland; and (B) detect and identify threats of terrorism against the United States;
- to disseminate, as appropriate, information analyzed by the Department within the Department, to… State and local governments and private sector entities with such responsibilities in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States.

- to request additional information from… State and local government agencies, and the private sector relating to threats of terrorism in the United States, or relating to other areas of responsibility assigned by the Secretary, including the entry into cooperative agreements through the Secretary to obtain such information.
- to coordinate with elements of the intelligence community and with Federal, State, and local law enforcement agencies, and the private sector, as appropriate.
- to perform such other duties relating to such responsibilities as the Secretary may provide.

Intelligence analysts from I&A and other DHS Components are expected to limit their activities in fusion centers to authorized intelligence activities, which have been defined under the I&A Interim Intelligence Oversight Guidance as relating to:

1. Terrorism and Terrorism Related Activities,
2. Other Threats to the Homeland,
3. Support to a Component of DHS,
4. Support to or Activities Directed by the Secretary, and
5. Activities directed by Statute or Presidential Directive.

Primarily I&A analysts will conduct activities under the first category.

By specifying purposes for which DHS may collect PII through the State and local fusion center program, DHS is reducing the risk of the program collecting information outside of its authority. DHS has put in place procedures so that internal and external reviewers can readily ascertain the reason information was collected, identify concerns, and confirm whether the information was collected within the scope of the program. Additionally, I&A operates under Executive Order (EO) 12333, *United States Intelligence Activities*. This EO applies to all members of the Intelligence Community and implements many of the FIPPs in a number of ways. Under DHS' implementing procedures for EO 12333, for instance, all I&A analysts must regularly review the information related to US Persons[19] that they maintain to ensure that it is necessary to conduct an authorized I&A intelligence activity, and that it remains relevant and timely. This supports purpose specification, among other FIPPs, by ensuring that the information is still relevant to the purpose for which it was collected over time.

Similarly, the ISE requires fusion centers to adopt and adhere to written privacy policies that establish policies and procedures ensuring that access to and use of PII is consistent with the

[19] United States person means a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. EO 12333 Section 3.4(i).

authorized purposes of the ISE. In addition, their written policies should include an assessment of their rules in order to ensure PII is collected only when it is legally permissible to do.

Fusion center compliance with 28 CFR Part 23 already implements this purpose specification principle in a number of ways: First, such fusion centers may not place information into a covered system that is obtained in violation of any applicable Federal, State, or local law or ordinance. In addition, since the purpose of these systems is to maintain criminal intelligence information, the Part explicitly limits the information States may place into the system to criminal intelligence information concerning an individual where there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.

4. Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish specific lawful purpose(s) and only retain PII for as long as necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

It is certainly true that fusion centers will collect information about US Persons. Clear policies for review of US Person information, as well as technical support, are in place to allow I&A representative in fusion centers to minimize the amount and type of US Person information that is collected, used, maintained, and disseminated. For instance, where a law enforcement officer seeks PII from I&A, he or she must be able to demonstrate a reasonable suspicion of criminal activity that may lead to terrorism. Where that showing cannot be made, the I&A analyst will only share activity-based information, stripped of PII. This, in conjunction with the previously mentioned mandatory reviews of US Person holdings, means that information is reviewed to ensure that only the minimum is disseminated.

EO 12333, in particular, implements the data minimization principle in several ways. First it limits the character of PII about US Persons I&A may collect, maintain, or disseminate, to:[20]

(a) Information that is publicly available or collected with the consent of the person concerned;

(b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations.

(c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international narcotics or international terrorism investigation;

[20] EO 12333 Section 2.3, Collection of Information.

(d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims or hostages of international terrorist organizations;

(e) Information needed to protect foreign intelligence or counterintelligence sources or methods from unauthorized disclosure.

(f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;

(g) Information arising out of a lawful personnel, physical or communications security investigation;

(h) Information acquired by overhead reconnaissance not directed at specific United States persons;

(i) Incidentally obtained information that may indicate involvement in activities that may violate federal, state, local or foreign laws; and

(j) Information necessary for administrative purposes.

28 CFR Part 23 implements the data minimization principle in fusion centers operating criminal intelligence systems by requiring a reasonable suspicion that the information relates to an individual involved in criminal conduct activity, and that the information is relevant to that conduct or activity; and, prohibiting the collection of information about the political, religious or social views, associations, or activities of any individual or any group, unless that information directly relates to criminal conduct and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity. In addition, it provides a measurable standard for establishing the necessary reasonable suspicion or criminal predicate before information is placed into the criminal intelligence system.

5. Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose that complies with the purpose for which the PII was originally collected.

As noted, information sharing with State and local law enforcement entities, as well as appropriate private sector entities, is a stated purpose of the HSIN Database privacy compliance documentation. Similarly, the System of Records for the I&A Enterprise Records System,[21] provides notice regarding the information sharing that can and will occur between I&A, other DHS components, State and Local fusion centers, and others protecting the homeland. The sharing occurs within the general confines of a nexus to terrorism and protecting the homeland. Any

[21] Enterprise Records System, DHS/I&A – 001, published May 15, 2008, 73 FR 28128.

sharing that occurs is recorded so that reviews can be conducted to ensure that sharing is occurring within the confines of the published notices.

As noted previously, State and Local Fusion Center I&A employees generally have access to HSIN database information. Information derived from TECS may also be provided to such employees as appropriate and shared in accordance with the published Privacy Act routine uses. Instances of sharing from TECS are logged for later review Any other systems that State and Local Fusion Center I&A employees may gain access to will be reviewed and appropriate sharing procedures and associated training will be put in place.

The Global Guidelines, further, state that the subsequent use of information should be compatible with the specified purpose. The Privacy Office anticipates that the fusion centers' written privacy policies will reflect this commitment.

Under 28 CFR Part 23, States already implement this FIPP by sharing information only when there is a need and a right to know the information in support of a law enforcement activity. In addition, fusion center personnel may only share information held in covered systems where the recipient agrees to follow the procedures regarding information receipt, maintenance, security, and dissemination consistent with the Part.

6. Data Quality and Integrity

Principle: DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

I&A analysts assigned to fusion centers are required to follow EO 12333 and DHS' interim implementing guidance. These authorities implement this principle by requiring regular review of information on US Persons to ensure it is still required, timely and relevant.

The ISE Privacy Guidelines require DHS and other Initiative participants to adopt and implement procedures to prevent, identify, and correct errors in protected information. ISE member are expected to communicate with other members when errors are discovered, even if they are merely the recipients of the information. Additionally, ISE members, including the fusion centers, may retain information only so long as it is relevant and timely.

Fusion centers complying with 28 CFR Part 23 are already familiar with this concept as they are prohibited from collecting and maintaining information on a Federally-funded criminal intelligence system unless it is relevant to criminal conduct or activity. Operators must periodically review information and delete that which is misleading, obsolete or unreliable. When doing so, they must provide notice to recipient agencies of any such revisions. Reviews must be auditable, and must include the reviewer's name, date of review, and an explanation why the information will be retained. Relevance is further assured by requiring information to be purged after five years.

These processes for criminal intelligence systems will translate well into fusion centers' general practices. The Global Guidelines encourage the centers to establish a business practice of notifying information sharing partners of inaccurate information and recommend limiting collection of information to that which is relevant to the purpose, accurate, complete, and up to date.

7. Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

For DHS, the HSIN database PIA describes the security safeguards built into the system to prevent loss or unauthorized use including access controls, registration eligibility, and heightened requirements where PII is involved. These security measures were sufficient to grant the HSIN Database system Certification and Accreditation (C&A) under the Federal Information Security Management Act (FISMA).[22] The C&A has been renewed based on updates to the system.

These existing safeguards are sufficient to satisfy the ISE Privacy Guidelines requirement that I&A use appropriate physical, technical, and administrative measures to safeguard protected information from unauthorized access, disclosure or destruction. A key aspect to security is ensuring that the roles and rules associated with access to the system are properly vetted. This provides the technical means to demonstrate who has access to what information and is integral to any information sharing environment.

States' experience with 28 CFR Part 28 will also serve as the basis for complying with ISE requirements in their fusion centers. Compliance requires fusion centers to ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to ensure against unauthorized access and against intentional or unintentional damage. The Global Guidelines recommend, in addition to taking steps to prevent unauthorized use, that fusion centers explicitly recognize an overlap between security procedures and privacy protection. They also encourage fusion centers to develop a consistent sanction policy for failure to comply with their privacy policies, that applies equally to all individuals in the organization.

8. Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

On the Federal side of the Initiative, the HSIN Database PIA details the important role that access and security audits play in the protection of privacy within the system. For I&A analysts assigned to fusion centers, moreover, DHS instituted a process by which information collection and sharing is logged with information regarding why the information was collected, and under

[22] 44 U.S.C. § 3541, *et seq.*

what authority. Information about any dissemination is similarly logged. This will allow DHS to review and verify that information is handled in accordance with the FIPPs, the Privacy Act, EO 12333, and DHS's interim implementing guidance for EO 12333.

State practitioners operating under 28 CFR Part 23 are also familiar with stringent audit requirements. Operators of criminal intelligence systems, like most fusion centers, must also create business processes which make auditing easier, including documenting the names of individuals who access information, the date of access, and the purpose. They must also add auditable statements of determinations of continued relevance.

Where gaps exist, the Global Guidelines make a number of recommendations to enhance accountability in their systems. For instance, fusion centers are encouraged to eliminate unnecessary discretion in decision making, and guide necessary discretion; develop and enforce a consistent sanction policy; follow all local breach notification laws; and provide adequate training, and regular privacy audits.

Fusion Centers and Privacy Concerns

Despite implementation of the FIPPs, fusion centers engender a range of concerns about privacy, from broad mischaracterizations of them as "mini-spy agencies," reminiscent of the most offensive domestic overreaching by the Federal Government in the 1960s and 70s, to more focused concerns about the privacy implications of sharing PII across the expansive fusion center network. The Privacy Office employed a number of sources to catalogue and understand the privacy concerns expressed about the fusion center model. For instance, there are a number of published reports—authored by both the Government and the privacy advocacy community—addressing privacy issues in fusion centers.[23] Also, as mentioned above, the Privacy Office has toured fusion centers around the country, participated in a number of fusion center conferences, met with representatives from the privacy advocacy community, and held a public meeting of the DPIAC committee to hear testimony about privacy issues surrounding the Initiative.

In the course of these efforts, the Privacy Office identified a number of risks to privacy as well as the steps DHS and individual fusion centers have taken to mitigate those risks. This section will examine these issues and explain the mitigation strategies for those risks, giving life to the FIPPs. Where necessary, the Privacy Office will offer recommendations on how DHS (and individual fusion centers) can take additional action to further enhance the privacy interests of the citizens they are charged with protecting.

[23] See, e.g., CRS and GAO reports (supra, note 15); American Civil Liberties Union, *What's Wrong with Fusion Centers*? Washington, 2007, ACLU.

1. Justification for Fusion Centers

The 9/11 Commission Act formally codified and established the fusion center Initiative; The Concept of Operations, to which this PIA is attached, is the fullest statement of the program's authority and justification.

Nonetheless, it should be noted that some non-governmental reviewers have expressed a concern that, despite clear statutory authority, unresolved privacy issues could threaten the program. In its report on fusion centers, CRS generally identified privacy violations as a potential risk to the fusion center concept. The Privacy Office recognizes this; frequent and serious privacy violations will erode public confidence in the important purposes of the Initiative. The CRS report recommended enhanced privacy training as a means of maintaining public confidence that fusion centers are protecting individual privacy. This need for training was echoed in GAO's report on fusion centers. The Privacy Office believes the training required by the 9/11 Commission Act—for I&A personnel and State and local fusion center representatives—as well as the guidance issued by the PM-ISE, will promote all of the FIPPs, by enhancing awareness and understanding of the FIPPs, and by assisting fusion centers to create the policies and documentation that give expression to their own application of the FIPPs.

Moreover, the Privacy Office is committed to working with SLPMO to assist the public in understanding Departmental programs. This PIA, as well as the public DPIAC meeting on fusion centers, and information exchanges between I&A fusion center managers and the privacy advocacy community are important actions that should serve as a model for future engagements. It is also worth noting that Global's Fusion Center Guideline Three, which DHS endorses, recommends that individual fusion centers establish a privacy committee responsible for, among other things, enhancing transparency through liaising with their local privacy advocacy communities. Also, to the extent possible, the Privacy Office encourages fusion centers to make their written privacy policies and other governance documentation available to the public. These privacy policies, and recommended State-drafted PIAs, should adhere to the guidance of the PM-ISE, and should include a description of the steps the center is taking to apply the FIPPs to their own operations.

Compliance with the FIPPs begins with Transparency. Regular and aggressive public accounting of fusion center activities is the best means to ensure continued public support for the fusion center Initiative.

2. Ambiguous Lines of Authority, Rules, and Oversight

GAO identified confusing lines of authority and the absence of clear rules as a concern in its report, as well. Nearly ten percent of the fusion centers interviewed by GAO were concerned about the lack of guidance on privacy while sharing or storing information.

In one sense, this is the natural consequence of combining Federal and State authorities governing coordinated efforts in most fusion centers. Federal employees assigned to fusion centers are subject to the Privacy Act of 1974, and are responsible for adhering to their Agency's

privacy policies, including application of the mandates of the PM-ISE. State and local employees, on the other hand, are responsible for adhering to their own State laws and policies, including those relating to the protection of individual privacy. These laws and policies should be addressed within each fusion center's written privacy policy. Moreover, these policies should be consistent with the guidance issued by the PM-ISE, and to the extent possible clearly delineate authorities for each fusion center participant to eliminate the potential for "policy shopping" raised by one critic.

Training provided by DHS, DOJ and the PM-ISE will mitigate this concern. In particular, the principles of Purpose Specification and Use Limitation require fusion center participants to understand their own authorities to undertake any action, including the collection and sharing of any PII. In addition, the documentation required by the PM-ISE will help clarify the centers' authorities and privacy responsibilities.

The principle of Accountability requires that the fusion center Initiative adhere to these authorities and privacy policies. At this time, fusion centers are engaged with DOJ BJA to draft their privacy policies. When they are finalized and in place, they will become the standard against which fusion centers can monitor their own actions. In addition to this internal review, the Initiative is subject to external oversight provided by Congress and GAO, the DHS and DOJ Offices of Inspector General, as well as the DHS Privacy Office (and Office for Civil Rights and Civil Liberties) and DOJ's Privacy and Civil Liberties Protection Office. The fusion centers themselves, moreover, are subject to the oversight mechanisms in place within their own States.

As noted above, State practitioners operating under 28 CFR Part 23 are already subject to robust audit requirements and must create business processes making auditing easier. The Global Guidelines make a number of recommendations to enhance accountability in their systems, as well, including a requirement for regular privacy audits.

3. Participation of the Military and the Private Sector

Concern about military participation is beyond the scope of this PIA.[24] Of course, each fusion center and Federal participant is encouraged to review and understand its authority to participate as a first step in preparing its foundational documentation.

The privacy concerns raised by private sector participants in fusion centers can be mitigated by formally restricting the amount of PII shared with private sector representatives, consistent with both the Use Limitation and Data Minimization principles. It is well understood that, for a variety of reasons, many fusion centers have moved to an all-hazards mission. This includes infrastructure protection. Since a large majority of critical infrastructure is owned by the private sector, certain information is necessary to assist owner-operators in understanding various threats against them, but it is not clear that such information must include PII. Also, this concern extends to the opposite information flow: from the company to the fusion center. While the

[24] We do note, however, that consideration of the military's role must begin with the particular military unit and the authority under which it operates. State National Guard units operating under state law or in a Title 32 status may have greater latitude than do active duty military units in a Title 10 status.

privacy implications of this bear examination, the CRS report, for instance, states that there is "a misconception that fusion centers… have access to vast amounts of private sector data. This is largely unfounded."[25] The Privacy Office will revisit this issue when this PIA is updated and in our follow-up report on the Initiative required by the 9/11 Act.

4. Data Mining

Some program reviewers are concerned that fusion centers will conduct unchecked data mining, equating the term "data fusion" with "data mining." Although the Homeland Security Act of 2002 requires the Department to utilize data mining, the term is not well understood by the public, and the Privacy Office acknowledges that data mining may raise privacy concerns. Each year, DHS reports on its data mining activities, applying a definition supplied by Congress. Reports for 2006, 2007, and a letter report for 2008 are on the Privacy Office's public facing website, www.dhs.gov/privacy. A data call is underway for an update to the 2008 report. Later in the year, the Privacy Office will conduct a public data mining workshop to explore validation models for data mining and privacy-enhancing technologies such as anonymizing and auditing tools.[26] The Privacy Office will update this PIA as it learns more about fusion center data mining activities.

5. Excessive Secrecy

This concern is responsible for the mischaracterization of fusion centers as mini-spy agencies or akin to the FBI's discredited—and long abandoned—COINTELPRO program. First, the SLFC PMO can reduce the potential for abuse by encouraging the centers to develop and adhere to a written privacy policy, one of the principle privacy protections identified by the PM-ISE. A well written privacy policy will force fusion centers to examine and document their legal authorities for undertaking various activities. It will then become the standard to which they train and hold their employees. This will significantly reduce the likelihood that centers will use their powers inconsistent with their authorities. These requirements are already imposed on States as part of 28 CRF Part 23, which expressly prohibits users of Federally-funded criminal intelligence systems from collecting information about the political, religious or social views, associations, or activities of any individual or organization unless such information directly relates to criminal conduct or activity.

Of course, general fears of excessive secrecy are best allayed by fully implementing the Transparency principle. As this PIA repeats a number of times, fusion centers are encouraged to publish their privacy compliance documentation, including an individualized PIA; establish a privacy committee to interact with their local privacy advocacy communities; and to listen to and address concerns whenever possible. When mistakes are made, the Privacy Office recommends

[25] CRS Report at 29.
[26] Both the Data Mining Workshop and 2008 Data Mining Report are now complete. Details about the workshop and a copy of the report are available on the DHS Privacy Office's website, www.dhs.gov/privacy. There are no instances of data mining relating to fusion centers discussed in the report.

that Initiative participants acknowledge the error and take corrective action, both to mitigate the harm and reduce the possibility of a recurrence. In addition to Transparency, this will promote Accountability and, ultimately, the rest of the FIPPs.

6. Inaccurate or Incomplete Information

The Privacy Office acknowledges that the more widely information is shared, the greater the possibility that incorrect or incomplete information will have negative consequences for individuals. In addition, the ability of an individuals to successfully correct errors is constrained the further the information travels from the source agency.

To help mitigate this concern, the PM-ISE is issuing guidance that fusion centers (a) establish accuracy procedures to help prevent, identify, and correct errors in PII; and (b) provide error notice to the privacy official of the source agency; adopt and implement ISE policies and procedures for the merger of information, investigation, and correction/deletion/nonuse of erroneous or deficient information, and retain PII only as long as it is relevant and timely, closely tracking requirements under the Privacy Act and EO 12333. Successful development and implementation of these policies will help promote the Data Quality and Integrity FIPP. While this is a significant challenge for a broad network of fusion centers, it must be noted that fusion centers are already practiced in regularly reviewing and purging incorrect or stale information held in their Federally-funded criminal intelligence systems, in order to be compliant with 28 CFR Part 23.

Of course, the Privacy Office also recognizes that the principle of Individual Participation plays a significant role in data quality issues. Specifically, allowing individuals to seek redress to correct erroneous information about them held in a system is recognized as an important privacy protection. Accordingly, the PM-ISE is issuing guidance that fusion centers establish procedures to address complaints about the use of PII under the fusion center's control. This redress, together with the requirement to provide error notice to the source agency, should mitigate the extent of the impact of incorrect or untimely information.

7. Mission Creep

It is widely acknowledged that fusion centers have expanded beyond their first mission. As the CRS report states on its first page: "Although many of the centers initially had purely counterterrorism goals, for numerous reasons, they have increasingly gravitated toward an all-crimes and even broader all-hazards approach." This observation is preceded in the report by one of the more obvious of the numerous reasons they might have cited: "Fusion centers are state-created entities largely financed and staffed by states…" Importantly, that sentence ends, "… and there is no one 'model' for how a center should be structured."

The Department must acknowledge that there are many possible fusion center configurations and missions, and States are free to deploy their resources utilizing their own best judgment, beginning with their voluntary participation in the fusion center Initiative. Fusion

centers are encouraged here and by the PM-ISE to ensure that the missions they undertake match both their own legal authorities and their foundational documents, including their privacy compliance documentation. This will promote the principles of Transparency and Purpose Specification. A fusion center's decision to include an all-crimes or all-hazards approach, however, is beyond the proper scope of this PIA.

Of course, despite State provenance and control of individual fusion centers, the presence of DHS analysts within necessitates a substantive examination of threats to privacy associated with mission creep. For DHS, the mission refers solely to the authorities governing DHS participation. That mission is specifically framed by the responsibilities enumerated for the Department and analysts in the 9/11 Commission Act. More broadly, I&A and its analysts are responsible for working within the authorities provided in Title II of the Homeland Security Act, EO 12333, and the Interim Intelligence Oversight Guidance, discussed above.

Therefore, regardless of the approach chosen by any particular fusion center, DHS must ensure its analysts assigned to fusion centers support the I&A mission as defined explicitly by the Homeland Security Act. This, too, supports the principles of Transparency, Purpose Specification, and Use Limitation. In practice, this means DHS analysts will not share or collect information that does not have a nexus to DHS' mission and I&A's responsibilities; State crimes like larceny and assault may have a place in the fusion center, but DHS generally does not have a role in supporting their investigation.

Privacy Office Follow Up

This PIA is neither the beginning nor the end of the Privacy Office's engagement with the fusion center Initiative. Looking forward, the Privacy Office will continue developing and providing training to DHS personnel assigned to fusion centers, to State and local fusion center representatives, as well as to participants in the ISF and ITACG programs. In addition, the Privacy Office will continue to examine the program and monitor progress of program participants, and report our findings in an updated PIA.

The Privacy Office regularly reviews and revises PIAs as we learn more information about a program or program changes that impact individual privacy. Moreover, in this case, Congress mandated that the Privacy Office issue a report on the privacy impact of the Initiative one year after the passage of the 9/11 Commission Act. Although that time is approaching, the Privacy Office anticipates a number of things will happen in fusion centers in the interim which will supplement the information in this PIA. For instance, the Privacy Office anticipates visiting a number of additional fusion centers over the year as we deliver privacy training—each visit adds to our understanding of the particulars of individual fusion centers; in a year, more DHS analysts will be assigned to fusion centers; and the ISE guidelines for fusion centers will issue, and the fusion centers will be well on the way to creating the procedures necessary to fulfill the

requirement that their privacy protections are at least as comprehensive as the Federal members of the ISE.

The next Privacy Office report on the fusion center Initiative will focus on these developments, as well as examine the steps the participants have taken to mitigate the risks to privacy outlined above. No doubt additional risks will be identified. The Privacy Office is committed to working with Initiative participants to continuously monitor and enhance the privacy protections in place, giving the fullest expression to the FIPPs.

Conclusion

Fusion Centers involve information sharing in two directions, by and between the State and various Federal partners, including the FBI and DHS. Some fusion centers existed before the terrorist attacks on the Nation of September 11, 2001, and others came into existence as a response to that attack. The Department of Homeland Security established relationships with these fusion centers in order to make them a focal point for certain of its information-sharing responsibilities under the Homeland Security Act. Congress then established the Federal, State, Regional, and Local Fusion Center Initiative as part of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, in order to facilitate and stimulate bi-directional information flows using the established channels. These existing channels are the subject of prior PIAs, which identify the risks to personal privacy and examine the steps the participants have taken to minimize those risks.

Congress also established the Information Sharing Environment, and directed the Executive Branch to disseminate procedures for sharing Homeland Security Information. The Program Manager for the ISE has done so, including those relating to preserving privacy. Many fusion centers have grasped the importance of incorporating privacy protections into their procedures and have responded positively to the technical assistance offered by BJA (and supported by the DHS Privacy Office) on crafting a written privacy policy. The Privacy Office is also teaming with the DHS Office for Civil Rights and Civil Liberties to provide privacy, civil rights and civil liberties training to I&A analysts to be assigned to fusion centers as well as an introduction to these topics to State and local representatives within the fusion centers. We hope that this training will increase understanding of the privacy risk inherent in fusion center operations, reinforce knowledge of the FIPPs, and help fusion center personnel understand their responsibilities to protect individual privacy.

No information sharing regime is free from privacy risks. This PIA examined a number of these risks and the positive steps both the DHS participants in the Initiative as well as representatives of fusion centers have taken or should take in the future to mitigate them. As the program matures, the Privacy Office anticipates discovering new privacy challenges that need to be addressed. Accordingly, this PIA will be updated whenever necessary to reflect new understanding of the operation of fusion centers and the Department's interaction with them. Finally, the Privacy Office supports a regular and ongoing examination of privacy issues within the fusion centers

themselves. This should include conducting their own PIAs to understand the processes and authorities unique to their jurisdictions.

Responsible Officials

Robert Riegle
Director
State and Local Program Managers Office
Intelligence and Analysis
Department of Homeland Security
(703) 235-0760

Approval Signature

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

Appendix of Authorities and Materials

1. 28 CFR Part 23, 2007. Criminal Intelligence Systems Operating Policies.

2. American Civil Liberties Union, 2007. What's Wrong with Fusion Centers? Washington, ACLU.

3. Bureau of Justice Assistance, 2005. Intelligence-Led Policing: The New Intelligence Architecture. Washington, BJA.

4. Carter, David L., 2004. Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies. Washington, COPS.

5. Committee on Homeland Security, U.S. House of Representatives, 2006. State and Local Fusion Centers and the Role of DHS. 2007, GPO.

6. Congressional Research Service. 2007. Fusion Centers: Issues and Options for Congress. Washington, CRS.

7. Executive Office of the President. 2003. E.O. 13311, Homeland Security Information Sharing. Washington, Federal Register.

8. Executive Office of the President. 2003. E.O. 13356, Strengthening the Sharing of Information to Protect Americans. Washington, Federal Register.

9. Executive Office of the President. 2003. E.O. 13388, Further Strengthening the Sharing of Information to Protect Americans. Washington, Federal Register.

10. Forsyth, William A., 2005. State and Local Intelligence Fusion Centers: An Evaluative Approach in Modeling a State Fusion Center. Monterey, NPS.

11. Global Justice Information Sharing Initiative, United States Departments of Justice and Homeland Security, 2006. Executive Summary, Fusion Center Guidelines. Washington, BJA.

12. Global Justice Information Sharing Initiative, United States Departments of Justice and Homeland Security, 2006. Executive Summary, Fusion Center Guidelines. Washington, BJA.

13. Global Justice Information Sharing Initiative, United States Departments of Justice and Homeland Security, 2007. Fusion Center Privacy Policy Development, Privacy, Civil Rights, and Civil Liberties Policy Template. Washington, BJA.

14. Global Justice Information Sharing Initiative, United States Department of Justice, 2005. Executive Summary, National Criminal Intelligence Sharing Plan. Washington, BJA.

15. Global Justice Information Sharing Initiative, United States Department of Justice, 2003. National Criminal Intelligence Sharing Plan. Washington, BJA.

16. International Association of Chiefs of Police, 2002. Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State and Federal Levels: Recommendations from the IACP Intelligence Summit. Alexandria, IACP.

17. International Association of Chiefs of Police, 2003. Criminal Intelligence Model Policy. Alexandria, IACP.

18. International Association of Law Enforcement Intelligence Analysts, Inc., 1997. Intelligence Led Policing: International Perspectives on Policing in the 21st Century. Lawrenceville, IALEIA.

19. Law Enforcement Intelligence Unit, 2002. Criminal Intelligence File Guidelines. Sacramento, LEIU.

20. Lessons Learned Information Sharing, 2005. LLIS Intelligence and Information Sharing Initiative: Homeland Security Intelligence Requirements Process. LLIS.

21. Manhattan Institute, 2007. Policing Terrorism Report No. 2, State Fusion Center Processes and Procedures: Best Practices and Recommendations. New York, Manhattan Institute.

22. National Commission on Terrorist Attacks Upon the United States, 2004. The 9/11 Commission Report. New York, W.W. Norton & Company.

23. National Governors Association Center for Best Practices, 2005. Issue Brief, State Intelligence Fusion Centers: Recent State Actions. Washington, NGA.

24. Program Manager, 2006. Preliminary Report on the Creation of the Information Sharing Environment. Washington, ODNI.

25. Public Law 107–56, 2001. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act Of 2001.

26. Public Law 107–296, 2002. Homeland Security Act Of 2002.

27. Public Law 108–458, 2004. Intelligence Reform and Terrorism Prevention Act of 2004

28. Rand Corporation, 2004. When Terrorism Hits Home: How Prepared Are State and Local Law Enforcement? Santa Monica, Rand.

29. Teufel, Hugo, 2007. Prepared Statement of the DHS Chief Privacy Officer Before the House Homeland Security Committee on March 14, 2007. Washington, DHS.

30. United States Congress, 2007. Public Law 110-53, Implementing Recommendations of the 9/11 Commission Act.

31. United States Department of Homeland Security, 2007. Transcript of Proceedings, DHS Data Privacy and Integrity Advisory Committee, Afternoon Hearing, September 19, 2007. Arlington, DHS.

32. United States Department of Homeland Security, Homeland Security Advisory Council, 2005. Intelligence and Information Sharing Initiative: Homeland Security Intelligence & Information Fusion. Washington, DHS.

33. United States Department of Homeland Security, Homeland Security Advisory Council, 2004. Intelligence and Information Sharing Initiative Final Report. Washington, DHS.

34. United States Government Accountability Office. 2007. GAO-08-35, Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers. Washington, GAO.