June 5, 2009

PRIVACY AND CIVIL LIBERTIES POLICY GUIDANCE MEMORANDUM

Memorandum Number: 2009-01

MEMORANDUM FOR: DHS Directorate and Component Leadership

FROM: Mary Ellen Callahan
Chief Privacy Officer

Timothy J. Keefer
Acting Officer for Civil Rights and Civil Liberties

SUBJECT: The Department of Homeland Security's Federal Information Sharing Environment Privacy and Civil Liberties Protection Policy

Background

The Federal Information Sharing Environment (herein referred to as the 'ISE') is designed to facilitate the sharing of terrorism information and weapons of mass destruction information, and homeland security information (herein referred to collectively as 'terrorism-related information') among all relevant entities through the combination of information sharing policies, procedures, and technologies.[1] The ISE serves the imperatives of enhanced information sharing to combat terrorism and protecting information privacy in the course of increased information access and collaboration across and among ISE participants. The President's Program Manager for the ISE issued the ISE Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the ISE (herein referred to as the 'Privacy Guidelines') which require relevant entities to have a written privacy protection policy that is at least as comprehensive as these guidelines. This document constitutes the Department of Homeland Security's (DHS) Federal ISE Privacy and Civil Liberties Protection Policy ("Policy").

Applicability

The Policy applies to "protected information," which the ISE defines as information about U.S. citizens and legal permanent residents that is subject to information privacy, civil rights, and civil liberties protections required under the U.S. Constitution and Federal laws of the United States. DHS has instituted a policy whereby any personally identifiable information (PII)[2] that is collected, used, maintained, and/or disseminated in connection with a mixed system[3] is treated as a system of records subject to the administrative protections of the Privacy Act regardless of whether the information pertains

[1] DHS shares non-terrorism related information with external parties to facilitate its all-hazards mission. DHS also shares information internally within DHS. However, this Policy pertains specifically to terrorism-related information sharing within the ISE.

[2] Personally identifiable information is defined as any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual. This definition applies regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., DHS employee, or contractor.

[3] A mixed system means any system of records that collects, maintains, or disseminates information, which is in an identifiable form, and which contains information about U.S. persons and non-U.S. persons. The mixed system policy is applied consistent with the Privacy Act's inapplicability to intelligence files and data systems devoted solely to foreign nationals or maintained for the purpose of intelligence activities made subject to the provisions and protections of Executive Order 12333. The mixed system policy does not establish a right of judicial review for nonresident aliens.

to a U.S. citizen, legal permanent resident, visitor, or alien.[4] As a result, this Policy also applies to information about nonresident aliens[5] contained in "mixed systems."[6]

The collection of protected information and information about nonresident aliens contained in mixed systems, including both that which originates from DHS and that obtained through the ISE shall be handled in accordance with this Policy. When DHS brings information about nonresident aliens into a mixed system, this information is treated in accordance with this Policy unless specific exceptions are negotiated in applicable information sharing agreements.[7] When DHS shares protected information and information about nonresident aliens contained in any of its mixed systems with ISE participants outside DHS, the information will be subject to the applicable protections of that recipient's written privacy protection policy, and any additional protections contained in negotiated information sharing agreements.[8]
This Policy also applies to agreements with international partners to the extent the information exchanged falls within the scope of the ISE.

For additional information about the Department's mixed system policy see *DHS Privacy Policy Guidance Memorandum 2007-01, Regarding Collection, Use Retention, and Dissemination of Information on Non-U.S. Persons*, January 7, 2009 (as amended from January 17, 2007).

Compliance with Laws and Identification of Protected Information
DHS only collects protected information and information about nonresident aliens contained in mixed systems when it has authority to do so. DHS complies with the Privacy Act of 1974, the E-Government Act of 2002, the Homeland Security Act of 2002, and other applicable laws regarding privacy, civil rights, and civil liberties and related Executive Orders. A number of official guidance documents issued by the DHS Privacy Office and the Office for Civil Rights and Civil Liberties, including those listed below ensure compliance with Federal privacy, civil rights, and civil liberties law and policy.

- *DHS Privacy Act Regulations*, January 27, 2003.
- *Management Directive 0470.2, Privacy Act Compliance*, October 2005.
- *Privacy Impact Assessments Official Guidance*, May 2007.
- *Privacy Technology Implementation Guide*, August 2007.
- *Privacy Incident Handling Guidance*, September 2007.
- *System of Records Notices Official Guidance*, April 2008.
- *Privacy Act Statements ((e)(3) Statements) Guidance*, April 2008.
- *Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS*, October 2008.

[4] Section 2.3 of Executive Order 12333 permits elements of the Intelligence Community to collect, retain, or disseminate information concerning U.S persons, which includes both U.S. citizens and legal permanent residents, but only in accordance with specific implementing procedures. Within DHS, these procedures require personnel to exercise due diligence in determining whether or not the subject of the intelligence is a U.S. person. When DHS conducts the necessary due diligence to identify whether or not the information in its intelligence systems is about a U.S. person, such systems are not considered mixed systems.
[5] Circular A-108, Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28, 948, 28951 (July 9, 1975). A nonresident alien is neither a U.S. citizen nor a legal permanent resident. For example, a nonresident alien could be a visitor or an alien.
[6] Nothing in this Policy should be interpreted as granting nonresident aliens whose information is contained in a mixed system with rights beyond the administrative protections of the Privacy Act such as access and correction, than were provided in the *DHS Privacy Policy Guidance Memorandum 2007-01, Regarding Collection, Use Retention, and Dissemination of Information on Non-U.S. Persons*, January 7, 2009 (as amended from January 17, 2007) (however this policy does not extend or create a right of judicial review for non-U.S. Persons). The term "Non-U.S. person" used in Policy Guidance Memorandum 2007-01 is synonymous with the term "nonresident alien" used in this Policy.

[8] DHS recognizes that ISE participants outside of DHS may not have a mixed system policy.

- *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*, December 2008.
- *DHS Policy Regarding Privacy Impact Assessments*, December 2008.
- *DHS Office for Civil Rights and Civil Liberties, Civil Liberties Impact Assessment Template,* December 2008.
- *Civil Rights and Civil Liberties Protection Guidance,* August 2008.
- *DHS Policy Against Racial and Ethnic Profiling*, 2004.
- *Management Directive 3500, Operational Roles and Responsibilities of the Officer for Civil Rights and Civil Liberties & the Office of the Chief Counsel,* May 2004.

For more information about how DHS complies with Federal privacy law and policy, visit www.dhs.gov/privacy. For additional information about how DHS complies with Federal civil rights and civil liberties protections and policy, visit http://www.dhs.gov/civilliberties.

Constitutionally Protected Activities
DHS is not authorized to collect or retain information solely for the purpose of monitoring activities protected by the U.S. Constitution, such as the First Amendment protected freedoms of religion, speech, press, and peaceful assembly and protest. If information has some connection to constitutionally protected activities, it may be collected only where such collection is incidental to the authorized purpose.

DHS is also not authorized to collect or retain information based solely on race, ethnicity, national origin, or religious affiliation. *See DHS Policy Against Racial and Ethnic Profiling, June 2004 (*adopting the *U.S. Department of Justice Guidance Regarding the Use of Race by Federal Law Enforcement Agencies, June 2003*.). If it is later discovered that information was collected and was subsequently disseminated, the originator should make reasonable efforts to ensure that recipients of the information are notified of the improper collection and delete or refrain from using the information.

Identification of Protected Holdings
System owners, in consultation with the DHS Privacy Office and Office for Civil Rights and Civil Liberties, are responsible for identifying data holdings that contain protected information and information about nonresident aliens contained in mixed systems. Once identified, system owners are further responsible for ensuring that information is made available to the ISE in accordance with this Policy.

Notice to ISE Participants
DHS components and system owners participating in the ISE will establish mechanisms for communicating information regarding the nature of the information made available to the ISE. These notice mechanisms will ensure that ISE recipients handle protected information and information about nonresident aliens contained in mixed systems in accordance with applicable legal requirements. This notice will, to the extent feasible, permit ISE participants to determine whether the information pertains to a U.S. citizen or legal permanent resident, is subject to specific information privacy or civil rights or civil liberties requirements, and has any limitations on reliability or accuracy.

DHS Fair Information Practice Principles
The FIPPs are a set of eight principles rooted in the tenets of the Privacy Act of 1974[9] and include: Transparency; Purpose Specification; Use Limitation; Data Minimization; Data Quality and Integrity; Data Security; Governance, Accountability and Auditing; and Individual Participation and Redress. The

[9] The Privacy Act of 1974, as amended 5 U.S.C. § 552a.

FIPPs form the basis of the Department's privacy and other civil liberties compliance policies and procedures governing the use of (PII), including this Policy.[10]

Transparency
DHS provides transparency about its ISE participation through various notice mechanisms, including the publication of this Policy, System of Records notices (SORNs), privacy impact assessments (PIAs), which are available[11] on the DHS Privacy Office website, http://www.dhs.gov/privacy, and civil liberties impact assessments (CLIAs), which are available on the DHS Office for Civil Rights and Civil Liberties website, http://www.dhs.gov/civilliberties.[12] DHS also promotes transparency regarding its ISE participation through its congressional testimony, public meetings of the DHS Data Privacy and Integrity Advisory Committee, and outreach to the privacy and civil liberties advocacy community.

Purpose Specification
DHS specifically articulates the authorities that permit the collection of protected information and information about nonresident aliens contained in mixed systems and clearly states the purposes for which the information is intended to be used in applicable SORNs, PIAs, and CLIAs. Planned uses, including sharing within the ISE must be compatible with the purpose for which DHS originally collected the information, both of which may be identified in SORNs, PIAs, CLIAs, laws, or information sharing agreements, as applicable. As noted in the February 1, 2007 DHS Policy for Internal Information Exchange and Sharing, all DHS components are considered part of one "agency" for purposes of the Privacy Act. Thus, sharing within DHS does not require a routine use, rather internal agency recipients must demonstrate a need-to-know for the record in the performance of their duties. Practices that support demonstration of a need-to-know may include requiring authentication of the users' need when accessing the information.

Use Limitation
Consistent with the Privacy Act and DHS SORN guidance, DHS uses protected information and information about nonresident aliens contained in mixed systems for the purpose(s) specified in its notices, and any sharing of such information outside the agency must be compatible with the purpose(s) for which the information was originally collected. DHS limits its use of protected information and information about nonresident aliens contained in mixed systems through sharing with ISE recipients to the extent that it is terrorism-related and an applicable authority permits such sharing. As a part of the DHS PIA process and addressed in PIA guidance, components must articulate the purpose and authorities for the collection of information as well as identify the internal and external recipients with whom they share PII.

DHS also has an agency-wide policy in place to limit its use of Social Security numbers. For more information see, *Memorandum Number 2007-02: Use of Social Security Numbers at the Department of Homeland Security*, June 4, 2007.

Data Minimization

---

[10] See DHS, *Privacy Policy Guidance Memorandum 2008-01:- The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (December 29, 2008).
[11] To the extent practicable, DHS makes its PIAs publicly available through its website, publication in the *Federal Register*, or by other means. Publication may be modified or waived for security reasons, or to protect classified, sensitive, or private information included in an assessment. These PIAs, while not made available to the public, are often made available for the Congress, the DHS Office of Inspector General, and other appropriate reviewers.
[12] To the extent practicable, DHS makes its CLIAs publicly available through its website. Publication may be modified or waived for security reasons, or to protect classified, sensitive, or private information included in an assessment. These CLIAs, while not made available to the public, may be made available for the Congress, the DHS Office of Inspector General, and other appropriate reviewers.

DHS only collects protected information and information about nonresident aliens contained in mixed systems that is relevant and necessary[13] to accomplish the purpose(s) specified in its notices and only retains such information for as long as is necessary to fulfill the purpose(s) specified in its notices. These practices are consistent with the Privacy Act and are reinforced by DHS SORN and PIA guidance.

When DHS shares protected information and information about nonresident aliens contained in mixed systems with ISE participants, it does so in a manner that minimizes its dissemination to that which is relevant and necessary to accomplish the ISE participant's request. Accordingly, DHS does not provide access to or disseminate DHS datasets in their entirety unless DHS determines that a dataset in its entirety is relevant and necessary to meet the request. Within the ISE, the information will be subject to the retention period defined by the DHS's privacy compliance documentation including applicable SORNs and PIAs covering the initial collection unless the information sharing agreements expressly modifies the retention period. For this reason, DHS Components should participate in the information sharing agreement process to ensure its data retention requirements are carried forward.

Data Quality and Integrity
DHS endeavors to use and share protected information and information about nonresident aliens contained in mixed systems within the ISE that is reasonably considered accurate and appropriate for their documented purpose(s), and to protect the integrity of the data. DHS takes a number of steps to address this:

- Upon receiving information from an ISE participant that DHS determines may be inaccurate, DHS will notify in writing the contributing agency's ISE Privacy Official.
- As outlined in this Policy, prior to making protected information and information about nonresident aliens contained in mixed systems available within the ISE, notice will be provided to the ISE recipients that will permit recipients to determine the nature of the information, including any limitations on the quality of the data.
- Should DHS determine that protected information and information about nonresident aliens contained in mixed systems that it originates is inaccurate or is erroneously shared, it will take appropriate steps to notify the ISE participant(s) who received the information and request the correction or deletion of the inaccurate data. Such notice may be provided in an information sharing agreement at the time of the agreement and on an ongoing basis in conjunction with the transfer of the information through use of cover memoranda.
- DHS also has redress mechanisms in place whereby subject to applicable and appropriate exemptions claimed for DHS systems of record under the Privacy Act, individuals may request correction of their data. For more information, please refer to the section on Redress**.**

Data Security
DHS employs measures designed to safeguard protected information and information about nonresident aliens contained in mixed systems from inappropriate, unauthorized, or unlawful access, use, disclosure, or destruction. DHS complies with the Federal Information Security Management Act of 2002 (FISMA),[14] and has implemented an information security program to ensure appropriate safeguards are in place. ISE recipients will be required to demonstrate compliance with FISMA. Additional information security requirements may be defined in information sharing access agreements.

Governance, Accountability and Auditing
The DHS Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties serve as the agency's ISE Privacy and Civil Liberties Officials and will provide guidance to components for implementing the DHS ISE Privacy and Civil Liberties Protection Policy. The DHS Chief Privacy Officer and the Officer

[13] Subject to applicable and appropriate exemptions claimed for DHS Systems of Record under the Privacy Act.
[14] Title III, E-Government Act of 2002, Pub. Law 107-347, 116 Stat 2899, 2946 (December 17, 2002).

for Civil Rights and Civil Liberties participate in DHS' Information Sharing Coordination Council, a Department-wide group administered by the Information Sharing and Collaboration (IS&C) Branch, Office of Intelligence and Analysis, and designed to provide coordinated, Department-wide deliberation and input on information sharing policy and related matters to the Information Sharing Governance Board (ISGB). The ISGB is, the executive steering committee and decision-making body for the Department on information sharing and collaboration issues. The ISGB oversees the planning and development of major information sharing programs and policies, and resolves internal information sharing and access disputes involving two or more DHS Components. Both the DHS Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties serve as *ex officio* members on the ISGB.

Outside the Department, the DHS Chief Privacy Officer is a co-chair of, and the Officer for Civil Rights and Civil Liberties is a member of the ISE Privacy Guidelines Committee, which issued and oversees the Privacy Guidelines on which this Policy is based and also coordinate with and the President's Privacy and Civil Liberties Oversight Board (PCLOB) concerning oversight of the Department's ISE activities.[15] Both the DHS Privacy Office and Office for Civil Rights and Civil Liberties provide the PCLOB and the Congress with quarterly reports on certain privacy activities pursuant to Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007 ("9/11 Commission Act").

DHS is committed to accountability for the acceptable use of protected information and information about nonresident aliens contained in mixed systems. DHS demonstrates accountability through a variety of mechanisms including those listed below.

- DHS provides transparency about its participation in ISE through various notice mechanisms including the publication of this policy, SORNs, PIAs, and CLIAs.
- DHS provides training to all employees and contractors who have access to or use PII.
- DHS provides training to DHS personnel and contractors and State and Local Fusion Centers regarding civil rights and civil liberties issues, including racial, ethnic and religious profiling.
- The Office for Civil Rights and Civil Liberties also offer several training products through its Civil Liberties Institute, available at http://www.dhs.gov/civillibertiesinstitute.com.
- DHS provides supplemental guidance including handbooks for handling and *Safeguarding Sensitive Personally Identifiable Information at DHS* and the *Privacy Incident Handling Guidance*.
- Additional role-based training is under development for those individuals who are authorized to handle protected information and information about nonresident aliens contained in mixed systems.
- DHS takes appropriate action when violations of its privacy policies are found.
    - Individuals who fail to implement safeguards will be held accountable through disciplinary or corrective actions. For additional information on the consequences and accountability for violation of federal laws, regulations, directives, or DHS policy, see *Privacy Incident Handling Guidance*.
    - Willful violation of the Privacy Act calls for criminal penalties for non-compliance and fines of up to $5,000 per violation.[16]
- CRCL reviews and assesses information concerning abuses of civil rights, civil liberties, and profiling on the basis of race, ethnicity, or religion, by employees and officials of the Department of Homeland Security.
- The DHS Office of Inspector General reviews DHS programs and activities to promote effectiveness and prevent abuse.

[15] Currently the PCLOB is administratively inactive.
[16] 5 U.S.C. § 552a(i).

To ensure implementation of the DHS Federal ISE Privacy and Civil Liberties Protection Policy, the DHS Office for Civil Rights and Civil Liberties and the DHS Privacy Office in conjunction with the component Privacy Offices periodically reviews DHS ISE policies and practices, including collection, access, use, disclosure, and destruction of covered information, to ensure such practices comply with this policy.

CRCL also periodically reviews certain programs and systems as part of its CLIA reviews and civil rights and civil liberties investigations.

Individual Participation and Redress
DHS has a number of redress mechanisms in place that provide individuals with opportunities to request access to their record(s), request correction of their record(s), and file a privacy or civil rights/civil liberties complaint Subject to applicable and appropriate exemptions claimed for DHS Systems of Record under the Privacy Act, available mechanisms are described below.

- *Access to DHS Records*
  Individuals seeking access to any record containing information that is part of a DHS system of records, or seeking to contest the accuracy of its content, may submit a Freedom of Information Act (FOIA) or Privacy Act request to DHS. Given the nature of some of the information shared through the ISE (sensitive law enforcement or intelligence information), DHS may not always permit the individual to gain access to or request amendment of his or her record. However, requests processed under the Privacy Act will also be processed under FOIA; requesters will always be given the benefit of the statute with the more liberal release requirements. The FOIA does not grant an absolute right to examine government documents; the FOIA establishes the right to request records and to receive a response to the request. Instructions for filing a FOIA or Privacy Act request are available at http://www.dhs.gov/xfoia/editorial_0316.shtm.

- *Travel-Related Inquiries*
  DHS has established the Traveler Redress Inquiry Program (DHS TRIP) to address perceived watchlist-related and other traveler screening redress inquiries. DHS TRIP is a Department-wide gateway to address watchlist misidentification issues; situations where travelers believe they have faced screening problems at ports of entry; and situations where travelers believe they have been unfairly or incorrectly delayed, denied boarding or identified for additional screening at our Nation's transportation hubs. Individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel may submit a redress inquiry online or by FAX or mail. Instructions for filing a redress inquiry are available at www.dhs.gov/TRIP.

- *Interagency Redress*
  The U.S. Terrorist Screening Center (TSC), charged with maintaining the U.S. government's consolidated terrorist watchlist, established a formal watchlist redress process. A Memorandum of Understanding (MOU) on Terrorist Watchlist Redress Procedures was agreed upon and signed by DHS and other agencies in September 2007. The MOU standardizes preexisting inter-agency watchlist redress procedures allowing individuals an opportunity to receive a timely, fair, and accurate review of their case. If DHS determines that an individual's adverse screening experience may be related to the terrorist watchlist it is referred to TSC's Redress Unit. TSC's Redress Unit follows written procedures to receive, track, and research watchlist-related complaints, to consult with agencies that nominate individuals to the watchlist, and to correct the watchlist or other data that may cause an individual unwarranted hardship or difficulty during a screening process. For more information on TSC redress visit: http://www.fbi.gov/terrorinfo/counterrorism/tsc.htm.

- *Civil Rights and Civil Liberties Inquiries*
  The Office for Civil Rights and Civil Liberties reviews and assesses information concerning abuses of civil rights, civil liberties, and profiling on the basis of race, ethnicity, or religion, by employees and officials of the DHS. If anyone (CRCL's complaint process is not limited to U.S. citizens, legal permanent residents, or nonresident aliens contained in mixed systems) believes that their civil rights or civil liberties have been abused, he or she may file a written compliant with the Office for Civil Rights and Civil Liberties. Instructions for filing a complaint are available at www.dhs.gov/CRCL.

- *Other Inquiries*
  Individuals who believe that their information may have been inappropriately shared within the ISE by DHS or who have other privacy complaints concerning DHS programs unrelated to travel may submit complaints to the Privacy Office at privacy@dhs.gov. Individuals may also submit complaints alleging abuses of civil rights and civil liberties or possible violations of privacy protections by DHS employees, contractors, or grantees to the Office of the Inspector General at DHSOIGHOTLINE@dhs.gov.

Implementation, Training, Technology

The DHS Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties are responsible for implementing the DHS ISE Privacy and Civil Liberties Protection Policy throughout the Department. This includes the development of training and review of applicable compliance documentation to ensure that if a proposed system or change to a system involves protected information and information about nonresident aliens contained in mixed systems, that it addresses the requirements of this policy. In addition to the annual mandatory privacy awareness training provided for all employees and contractors, the DHS Privacy Office is developing additional role-based training for agency employees involved in the development and use of the ISE. The Office for Civil Rights and Civil Liberties also offer several training products through its Civil Liberties Institute, available at http://www.dhs.gov/civillibertiesinstitute. DHS is also exploring the use of privacy enhancing technologies to facilitate accountability and implementation of this policy.

Information Sharing Access Agreements

The Department's information sharing activities with its external partners including other Federal agencies, State, local, Tribal entities, international partners, or the private sector that involve PII must be formally documented in an Information Sharing Access Agreement (ISAA). ISAAs are defined as any memorandum of understanding (MOU), memorandum of agreement (MOA), letter of understanding (LOU), letter of agreement (LOA), or any form of agreement that is used to facilitate the exchange of information between two or more parties. The ISAAs should address, at a minimum:

- applicable authorities for providing the information to the external recipient;
- applicable authorities for the recipient to collect the information;
- compliance with both DHS and ISE recipient privacy documentation including PIAs and SORNs;
- implementation of the DHS FIPPs; and
- acknowledge the parties are members of the ISE and that the parties' collection, use, maintenance and dissemination of PII under the agreement is consistent with each agency's written privacy and civil liberties protection policy.[17]

[17] DHS will share protected information and information about nonresident aliens contained in mixed systems with state, local and tribal governments, law enforcement agencies, and non-public entities that provide privacy protections at least as comprehensive and protective as those contained in the ISE Privacy Guidelines.

In addition, all ISAAs that include sharing of PII must be reviewed by the DHS Privacy Office, the Office for Civil Rights and Civil Liberties, and the Office of the General Counsel, and other relevant offices.

Appendix A - Definitions

Executive Order 12333 – As amended, lays out the goals, direction, duties, and responsibilities of all Executive Departments and Agencies with respect to U.S. intelligence efforts. The Order delineates the authorized roles and responsibilities of the Director of National Intelligence, the U.S. Intelligence Community, and each Department and Agency comprising an element of the Intelligence Community. The Order also directs that the Heads of all Executive Branch Departments and Agencies shall coordinate and collaborate with the DNI to address national intelligence requirements and provide the DNI access, as appropriate, to all information and intelligence relevant to the national security in accordance with guidelines to be approved by the Attorney General. Executive Order 12333 requires compliance with all applicable information sharing, security, privacy, and other legal guidelines.

Personally Identifiable Information (PII). DHS defines PII as any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a United States citizen, legal permanent resident, or a visitor to the United States. Examples of PII include: name, date of birth, mailing address, telephone number, Social Security Number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), Internet protocol addresses, biometric identifiers (e.g., fingerprints), photographic facial images, or any other unique identifying number or characteristic, and any other personal information that is linked to an individual.

Protected Information—The ISE defines protected information as information about U.S. citizens and legal permanent residents that is subject to information privacy or other legal protections under the U.S. Constitution and Federal laws of the United States. Protected information may also include other information that the U.S. government expressly determines (by Executive Order, international agreement, or other similar instrument) should be covered by these Guidelines. For the Intelligence Community, protected information includes information about United States persons as defined in Executive Order 12333, which provides that a U.S. person is 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. The definition of protected information may also include legal protections that are not strictly related to privacy. For example, information relating to the exercise of rights under the First Amendment may be subject to constitutional protections. Intelligence Community, information about U.S. corporations or associations that does not reveal personally identifiable information may nonetheless be subject to protection under Executive Order 12333. However, it is anticipated that in most cases, protections will focus on personally identifiable information about U.S. citizens and legal permanent residents.

Protected information to be made available within the ISE includes only that which is terrorism information, homeland security information, or weapons of mass destruction information which are defined as follows:

- **Terrorism Information**—Terrorism Information is defined in IRTPA Section 1016 (as amended) as all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to:

- The existence, organization, capabilities, plans, intentions, vulnerabilities, means of financial 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 of individuals reasonably believed to be assisting or associated with such groups or individuals.

It includes Weapons of Mass Destruction information.

- **Homeland Security Information**—Homeland Security Information, as derived from the Homeland Security Act of 2002, Public Law 107-296, Section 892(f)(1) (codified at 6 USC 482(f)(1)) is defined as any information possessed by a state, local, tribal, or federal agency that:
  - Relates to a threat of terrorist activity;
  - Relates to the ability to prevent, interdict, or disrupt terrorist activity;
  - Would improve the identification or investigation of a suspected terrorist or terrorist organization; or
  - Would improve the response to a terrorist act.

- **Weapons of Mass Destruction (WMD) Information-**– WMD Information is defined in Section 1016 of the IRTPA (as amended) as 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.

- **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." United States Intelligence Activities, Executive Order 12333. Section 3.4(i)

Appendix B - Expanded References

Legislation

Privacy Act of 1974 (5 U.S.C. § 522a, as amended).

E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch. 36).

Homeland Security Act of 2002 (Pub. L. No. 107-296, 116 Stat. 2135), as amended.

Federal Information Security Management Act of 2002 (44 U.S.C. § 3541).

Intelligence Reform and Terrorism Prevention Act of 2004, as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007 (50 U.S.C. § 402 et seq.).

Executive Orders

Executive Order 12333, *United States Intelligence Activities* (December 4, 1981, as amended).

Executive Order 13311, *Homeland Security Information Sharing* (July 29, 2003).

Executive Order 13353, *Establishing the President's Board on Safeguarding Americans' Civil Liberties* (August 27, 2004).

Executive Order 13356, *Strengthening the Sharing of Terrorism Information to Protect Americans* (August 27, 2004). (Rescinded)[18]

Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans* (October 25, 2005).

Policies, Guidance, and Other References

Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era, Global Justice Information Sharing Initiative, United States Department of Justice and Homeland Security, (August 2006).

Privacy Policy Guidance Memorandum 2007-01: DHS Privacy Policy Regarding Collection, Use, Retention and Dissemination of Information on Non-U.S. Persons, (January 19, 2007).

DHS Policy for Internal Information Sharing and Exchange (February 1, 2007).

Privacy Policy Guidance Memorandum 2007-02: Use of Social Security Numbers at the Department of Homeland Security, (June 4, 2007).

Privacy Incident Handling Guidance, (September 10, 2007).

National Strategy on Information Sharing, (October 2007).

[18] Section 3 of EO 13388 specifically refers to "common standards for the sharing of terrorism information established "pursuant to section 3 of EO 13356."

Privacy and Civil Liberties Policy Development Guide and Implementation Templates, Global Justice Information Sharing Initiative, Department of Justice, (February 2008).

DHS Information Sharing Strategy (April 18, 2008).

Civil Rights and Civil Liberties Protection Guidance, (August 11, 2008).