CIVIL LIBERTIES AND PRIVACY OFFICE
Implementation of the Information Sharing Environment
Privacy Guidelines for Sharing Protected Information
02 September 2009

PURPOSE

This privacy protection plan sets forth the mechanisms, policies and procedures the Office of the Director of National Intelligence (ODNI) will follow to implement the Information Sharing Environment (ISE) Privacy Guidelines, and governs how the ODNI, to include employees, detailees, assignees, contractors, and others who have access to ODNI information or systems that may be used in the sharing of terrorism-related information, shall handle records containing information about protected individuals (i.e., "protected information") when those records are disclosed to or received from other federal agencies; state, local, tribal and foreign terrorism information-sharing partners; and the private sector.

Processes outlined in this plan will assist the ODNI in complying with applicable privacy and civil liberties requirements with respect to sharing protected information, and with the safeguards for United States citizens and permanent resident aliens embodied in Executive Order 12333, and in guidelines and procedures implementing the provisions and protections of the Order.

AUTHORITIES

- The National Security Act of 1947, as amended;
- Executive Order 12333, as amended;
- Executive Order 13388;
- The Privacy Act of 1974, as amended; and
- Other applicable provisions of law.

REFERENCES

- Presidential Memorandum dated December 16, 2005 - *Guidelines and Requirements in Support of the Information Sharing Environment*;
- PM/ISE Memorandum dated December 4, 2006 - *Privacy Guidelines for the Information Sharing Environment*, and the attached *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment*;
- Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment dated September 10, 2007 and available at www.ise.gov.

- Intelligence Community Directive 102, *Process for Developing Interpretive Principles and Proposing Amendments to Attorney General Guidelines Governing the Collection, Retention, and Dissemination of Information Regarding U.S. Persons*.

DEFINITIONS

1. Information Sharing Environment (ISE): The ISE is an approach for sharing "protected information" contained in terrorism-related information (including information on weapons of mass destruction, homeland security information and law enforcement information related to terrorism) with federal, state, local, tribal, and private sector entities, as well as foreign partners. Mandated by Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), the ISE is composed of the policies, processes, protocols, and technologies that govern the handling and management of "protected information" subject to exchange with other entities. In practical effect, the term "ISE" refers to procedures for the sharing of terrorism information that contains information about protected individuals.

2. Protected Information: Protected information is information about United States citizens and permanent resident aliens that is subject to information privacy or other legal protections under the U.S. Constitution and federal laws. Protected information may also include information designated by Executive Order, international agreement or other instrument as subject to information privacy or other protections.

ROLES AND RESPONSIBILITIES

The ODNI shall ensure that information privacy, civil liberties, and other legal rights of United States citizens and permanent resident aliens are protected as terrorism-related information is exchanged between information-sharing partners.

The ODNI Civil Liberties Protection Officer (CLPO) is designated as the ODNI ISE Privacy Officer. In consultation with other responsible ODNI offices, the CLPO shall:

- Oversee the ODNI's implementation of and compliance with this plan;
- Ensure that policies, procedures and systems comply with this plan;
- Design, implement, and manage privacy and civil liberties training;
- Provide guidance for implementing this plan; and
- Review and assess complaints in accordance with the REDRESS section of this plan.

All ODNI components shall:

- Consult with the CLPO to determine the need to formalize a Standard Operating Procedure (SOP), which may be issued as an Internal Process Document (IPD), for implementing this plan. If an SOP is necessary, the component shall designate a senior official responsible for developing and implementing the SOP.
- Consult with the CLPO, when no SOP is needed, to ensure compliance with this plan.

- Ensure that protected information meets the standards of accuracy, completeness and consistency described in the DATA QUALITY section of this plan.

The Data Integrity and ISE Oversight Board shall evaluate components' processes and identify additional protections needed, as described within this plan.

PROCESS TO ENSURE COMPLIANCE WITH LAWS:

ODNI components seeking to share protected information with terrorism information sharing partners shall ensure that the protected information is subject to a thorough review of the privacy, civil liberties, EO 12333 guidelines and other applicable conditions and requirements for sharing ("ISE rules review," or "rules review."). Subject to further CLPO guidance, components shall:

- Consult with CLPO and other offices as CLPO may designate, (e.g., Office of the General Counsel, Mission Support Center/Information Management), document such consultations, and receive written affirmation from reviewing or consulting officials or offices that appropriate criteria have been met; or
- Prescribe an internal ISE rules review process as part of an SOP developed pursuant to the ROLES AND RESPONSIBILITY section of this plan and that meets with CLPO approval; and
- Document all data sharing between the ODNI and other entities via terms of reference, Attorney General Guidelines, Memoranda of Understanding (MOU) or similar instruments, and ensure review and approval of such documentation by the CLPO and other offices the CLPO may designate.

In conducting the rules reviews, CLPO, the Office of the General Counsel (OGC), and other relevant offices shall work with components to:

- Identify privacy, civil liberties, EO 12333 and other requirements that apply to the protected information to be shared;
- Develop guidance identifying any rules specific to particular sharing arrangements or categories of protected information; and
- Establish safeguards to ensure that protected information is not shared solely on the basis of the exercise of rights guaranteed by the First Amendment, or on the basis of race, ethnicity, national origin, or religious affiliation; and controls and limitations are implemented for protected information as applicable law or policy requires.

If, in conducting rules reviews, the CLPO, OGC, or any ODNI component identifies:

- An issue that erodes information privacy rights, civil liberties, U.S. person or other legal protections, the CLPO, upon identifying or receiving notice of such issue, shall initiate any internal reviews and policy processes needed to address the risk to protected rights or information;

- An internally imposed restriction on sharing protected information that impedes the sharing of terrorism, homeland security, or law enforcement information and that does not appear to be required by applicable laws or to protect information privacy, civil liberties, or other legal rights, the CLPO, upon identifying or receiving notice of such restriction, shall initiate any internal reviews and policy processes needed to address the apparent impediment; or
- A restriction of the type described in the above paragraph that is imposed by a requirement external to ODNI, the CLPO and OGC shall review such reported impediments, consult with the ISE Privacy Guidelines Committee and, failing internal resolution of the concern, bring such restriction to the attention of the Attorney General and the Director of National Intelligence pursuant to the ISE Privacy Guidelines.

CHARACTER OF DATA - NOTICE

ODNI components will provide a cover sheet or electronic banner, legend or screen notifying recipient agencies of the nature of the records, data, databases or systems of records, and appropriate approved control markings for unclassified information which they make available to other terrorism-related information sharing partners. The notice shall state whether the information:

- Contains protected information pertaining to a United States citizen or permanent resident alien, or a non-immigrant alien protected by treaty or international agreement;
- Is subject to legal restrictions on its access, use, or disclosure, and describes the restriction and pertinent law, regulation or policy; or,
- Is generally reliable and accurate. If its reliability and accuracy is unknown, describe the reason for limited confidence in source reliability or content validity (e.g., notice from previous recipient of data, independent review, inconsistency in records, etc.).

ODNI components shall also use the cover sheet or electronic banner, legend or screen to provide to the recipient agency POC pertinent contact information for the terrorism-related reports, records or data they disseminate. At a minimum, this information should include the name of the originating department or activity, and, if possible, the title and contact data for the person to whom questions regarding the information should be directed.

DATA QUALITY

The standards outlined below are the minimum required. ODNI components may impose stricter data quality standards.

Data Quality Reviews: Components shall ensure that protected information meets the standards of accuracy, completeness and consistency required to further the purpose(s) for which the information is collected and used. Specifically:

- To prevent, identify and correct errors, components shall conduct and document quality assurance reviews of protected data to the extent feasible, notwithstanding exemption from review under the Privacy Act of 1974 or other law;

- Components may document the decision that a data quality review conducted to satisfy a non-ISE legal or policy requirement (e.g., OMB mandate, term of MOU) is current and appropriate for the data set examined, recording date of review and legal authority/requirement for review;
- Components shall document a decision to review data sets in stages, based on priority areas or criticality of accuracy;
- Reviews may include comparison of records to detect inconsistencies or other concerns about accuracy.

Data Quality Processes: Components shall articulate processes and criteria to ensure:

- Merged/matched records relate to the same individual;
- Errors, inconsistencies and deficiencies are investigated and corrected/deleted in a timely manner;
- Outdated or irrelevant data is updated, deleted or segregated in a timely manner; and
- Data that is pending correction, updating, or deletion is withheld from disclosure or access or is appropriately segregated.

Notice of Errors in Data Received: When a component determines that protected information originating from an external source may be erroneous, includes incorrectly merged information, or lacks adequate context such that the rights of the protected individual may be affected:

- The potential error or deficiency shall be communicated in writing to the ODNI CLPO as well as to the other agency's ISE Privacy/Civil Liberties Official (identified in the applicable MOU or other instrument governing the information exchange); and
- The communication shall include information that clarifies, limits, contradicts or qualifies the information deemed to be erroneous or deficient.

Notice of Errors in Data Disseminated: When a component determines that protected information it originated is or may be erroneous or non-compliant with terrorism-related information sharing policy or other policy or statute, and knows or believes (based on logs/audit) that the information was accessed by another agency, the component shall take the following steps:

- Provide written notice to the ODNI CLPO of the deficiency, assessing the extent to which the protected information has been disseminated;
- Notify record recipients of the deficiency, if they can be identified, to include information that clarifies, contradicts or qualifies the deficient information;
- Correct or delete the erroneous information, or follow appropriate processes to dispose of the record. When it is uncertain whether the protected information is erroneous, note known limitations on accuracy in the field containing the protected information.
- Report the erroneous dissemination to the Intelligence Oversight Board and to the DNI as appropriate pursuant to Executive Order 12333.

Notice of Data Erroneously Shared: An ODNI component that shares protected information erroneously or in a manner that is inconsistent with this plan shall immediately:

- Recall the information by contacting all record recipients of the information and request immediate destruction of all disseminated copies of the information;
- Comply with ODNI guidance on managing breaches of personally identifiable information, and report the matter to the CLPO, who shall convene an Incident Response Team to evaluate the disclosure, decide if notice to record subjects is required, and, as needed, develop a response plan.

Data Integrity and ISE Oversight Board: As described in the ACCOUNTABILITY, ENFORCEMENT AND AUDITABILITY section of this plan, the Board will assess overall data quality and respond to identified data quality issues.

DATA SECURITY

An ODNI component sharing protected information through the ISE shall:

- Obtain assurances from the Mission Support Center (MSC) that MSC offices have implemented policies prescribing administrative, technical, and physical safeguards for protected information or will implement them soon. MSC policies should reflect, as applicable, the standards and directives in the Data Security sections of the Privacy and Civil Liberties Implementation Workbook for Federal Agencies.
- Coordinate with the ODNI/Chief Information Officer to implement appropriate privacy enhancing technologies including, but not limited to, permissioning systems, hashing, data anonymization, immutable audit logs, and authentication.

ACCOUNTABILITY, ENFORCEMENT AND AUDITABILITY:

ODNI components are responsible for cooperating with all ISE protected information audits and reviews conducted as set forth below. All completed reviews and audits shall be submitted to the CLPO.

ODNI CLPO shall establish a "Data Integrity and Oversight Board (Board)" with representation from each ODNI component that shares information through the ISE. The Board also shall include a representative from the IMO. The Board will oversee components' rules review and terrorism data inventory processes; examine data quality reviews to identify potential problem areas; and identify processes, policies or training to minimize the use or dissemination of erroneously protected information and to ensure that technical protections are implemented.

The ODNI CLPO shall work with components to implement audit procedures relating to the sharing of protected information with terrorism-related information sharing partners. Audits may be conducted on any or all of the elements addressed by the ISE Privacy Guidelines.

REDRESS

General: Components receiving requests for access to protected information, or complaints from individuals who believe protected information about them has been shared shall identify the

appropriate office through which to seek redress.

Requests for Access to ODNI Information: Responses to requests from individuals seeking access to protected information about them that is under an ODNI Component's control shall be addressed as prescribed by the ODNI's guidance on the Freedom of Information Act and Privacy Act Programs, and corresponding Privacy Act Regulations (32 CFR Part 1701). Such requests shall be forwarded to the ODNI's Office of Information Management, which will maintain a file of such requests and take action as appropriate.

Information Sharing Complaints, CLPO Role and ODNI Component Support:

- A component or ODNI redress action office that receives a complaint or allegation relating to the sharing of protected information shall promptly forward the complaint or allegation to the ODNI CLPO for acknowledgement, investigation and resolution as appropriate.
- CLPO shall be responsible for handling complaints or requests for redress involving terrorism-related information which are not identifiable as within the authority or responsibility of any of the other ODNI-internal offices.
- CLPO shall reconcile protocols for handling complaints arising, variously, under privacy and civil liberties authorities and under EO 12333, and ODNI components shall cooperate with procedures developed for conducting internal and external investigations and for communicating with complainants regarding the handling of all protected information.

Expungement: ODNI components receiving expungement orders issued by a federal court shall forward them to the OGC, with a copy to CLPO and MSC/IM. Components will coordinate with the OGC and IMO to comply with expungement orders and to determine how to respond to expungement orders issued by state courts.

Interagency Cooperation: Subject to DNI authorities, ODNI will respond as promptly as practicable to a request for information and cooperation from another agency to assist in addressing a complaint received by such other agency. ODNI, conversely, shall promptly request the assistance of other information sharing partners when a request is received that relates to the activities of the other partner in respect of terrorism-related information.

TRAINING

Privacy, civil liberties and U.S. person training will be mandatory for all personnel who collect, have access to, or disseminate protected information. The ODNI CLPO is responsible for designing, implementing, and managing this training.

The training program will, at a minimum, cover the following topics:

- Collection, retention, use, and dissemination of protected information;
- Reporting violations of privacy-protection policies; and
- Sanctions for misuse of protected data and non-compliance with this plan.

ODNI personnel who have access to protected information, or operate/maintain databases or National Security Systems, shall certify their participation in annual ODNI privacy, civil liberties and U.S. person training.

ODNI will provide training to ensure that all agency action offices possessing a redress function are familiar with ODNI's terrorism-related information sharing activities, and understand when a complaint or inquiry received implicates protected information subject to action by CLPO.

INTERNAL AWARENESS

The ODNI CLPO will facilitate appropriate awareness within the ODNI of policies and procedures for implementing this plan. The CLPO shall ensure that information about privacy, civil liberties and EO 12333 policies and procedures is updated as necessary.

NON-FEDERAL ENTITIES

To the extent consistent with applicable laws and guidance, the ODNI will share, as appropriate, terrorism, homeland security, and/or law enforcement information related to terrorism with state, local, and tribal governments, law enforcement agencies, and non-government entities providing they implement privacy protections that are at least as comprehensive as those prescribed by the ISE Guidelines. The Program Manager-Information Sharing Environment (PM-ISE) shall provide guidance on the privacy and civil liberties protection policies that non-federal entities should adopt in order to receive terrorism, homeland security and/or law enforcement information related to terrorism from federal terrorism information sharing partners.

The National Counterterrorism Center will facilitate the production of "federally coordinated" terrorism-related information for use by state, local, and tribal governments, law enforcement agencies, and non-government entities.

Components shall consult with the CLPO and with the Office of Policies, Plans and Requirements in anticipation of sharing terrorism information with non-federal entities.