DEPARTMENT OF THE INTERIOR
Privacy Policy for the Information Sharing Environment

September 30, 2009

Office of the Chief Information Officer

Version: 1.0.0

The Department of the Interior
ISE Privacy Policy

Version:	1.0.0
Date of Approval:	September 30, 2009
Effective Date:	September 30, 2009
Expiration Date:	When officially rescinded or revised
Originating Office:	Departmental OCIO
Point of Contact:	Pamala R. Quallich]
Distribution:	All Departmental Bureaus and Major Offices, And Senior Leaders throughout the Department
Intended For:	All Employees, Contractors, Volunteers, and the Public

---

Table of Contents

Background and Applicability 1

Compliance with Laws 2

Purpose Specification 6

Identification of Protected Information to be Shared Through the ISE 6

Data Quality 7

Data Security 7

Accountability, Enforcement and Audit 8

Redress 9

Execution, Training, and Technology 9

Awareness 10

Non-Federal Entities 10

Governance 10

General Provisions 10

Appendix A – Glossary of Acronyms 15

Appendix B – Version Control 16

Signature Section 17

The Department of the Interior
Privacy Policy for the
Information Sharing Environment

Background and Applicability.

a. Background. The Information Sharing Environment (ISE) is designed to facilitate access to terrorism related information by all relevant entities through a combination of information sharing policies, procedures, and technologies. In order to successfully implement the ISE, agencies must ensure that while meeting the goal of enhanced information sharing to combat terrorism, they ensure adequate protection of information privacy and the legal rights of U.S. citizens and lawful permanent residents.

The ISE is a core element of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).[1] Section 1016 required the creation of the ISE as an "approach that facilitates the sharing of terrorism information." Executive Order 13388 (October 25, 2005), "Further Strengthening the Sharing of Terrorism Information to Protect Americans," mandates that in the course of operating within the ISE, agencies shall protect the privacy rights of Americans. On December 16, 2005, to further the objectives of IRTPA and his Executive Order, the President issued a Memorandum for the Heads of Executive Departments and Agencies which set forth guidelines for the establishment, implementation, and operation of the ISE. Guideline 5 addresses privacy issues and required the Attorney General and the Office of the Director of National Intelligence to issue guidelines to all Executive Departments and Agencies regarding their protection of information privacy while participating in the ISE.

The ISE Privacy Guidelines (Guidelines) were published on December 4, 2006 by the ISE Program Manager. They establish the parameters of the ISE, and provide guidance on how Executive Departments and Agencies will share information in the ISE while ensuring that information about U.S. citizens and lawful permanent residents that is subject to information privacy or other legal protections under Federal law is protected from unnecessary disclosure. The Guidelines require each relevant entity in the ISE to have a privacy policy for the ISE. Accordingly, the Department has developed this ISE Privacy Policy.

b. Applicability. The Department of the Interior (DOI or the Department) ISE Privacy Policy applies to "protected information," which the Guidelines define as information about U.S. citizens and lawful permanent residents that is subject to information privacy, civil rights, and civil liberties protections under the U.S. Constitution and Federal laws of the United States, including, but not limited to, the Privacy Act, the E-Government Act, and the Federal Information Security and Management Act ("Protected information"). The Department has instituted a policy whereby any personally identifiable information (PII)

[1] *See 6 U.S.C. 485.*

that is collected, maintained, and/or disseminated in connection with a mixed system (a system containing protected information as well as privacy information about others who are not U.S. citizens or lawful permanent residents) is treated as a system of records subject to the administrative protections of the Privacy Act regardless of whether the information pertains to a U.S. citizen, legal permanent resident, visitor, or alien. As a result, this policy also applies to information about nonresident aliens contained in mixed systems.

This document constitutes the DOI ISE Privacy Policy. It is based on the framework established by the U.S. Constitution, Executive Orders 12333 and 13388, the Intelligence Reform and Terrorism Prevention Act of 2004, and the ISE Privacy Guidelines. All DOI employees, contractors and volunteers shall comply with the policy. Responsibility for its implementation rests with all those DOI employees, contractors, and volunteers accessing and using any ISE systems or information, and to all employees, contractors and volunteers, particularly law enforcement, the CIO, and senior management, as appropriate.

Protected information includes PII, 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. DOI will not share protected information through the ISE unless such information is terrorism, homeland security, or law enforcement information. The ISE Privacy Officials will issue internal procedures and protocols for Departmental employees involved in ISE sharing to ensure that its access to and use of privacy information is lawful. Further, the ISE Privacy Officials will provide oversight of such information to validate that all ISE activities conducted by the Department are in full compliance with legislation, including privacy legislation such as the Privacy Act.

Compliance with Laws.

a. *General.* With respect to privacy, it is the policy of the Department to comply with the United States Constitution, Executive Orders, the Privacy Act, OMB guidance, and all applicable legislation and guidance for Federal agencies.[2]

The Department has an ongoing legal responsibility to safeguard its information and to protect the privacy rights of citizens and lawful permanent residents. The privacy rights of citizens and permanent lawful residents derive primarily from the Privacy Act of 1974. The most important of these rights is the provision to have their personal privacy information kept confidential except where consent for release has been given, unless release of that information is authorized by law. Additional rights include the right to access such information about oneself and the right to institute corrective action when such information is inaccurate or incomplete.

[2] See DOI's Privacy Act regulations at 43 CFR Part 2, Subpart G, Sections 2.45 through 2.79, and other Departmental guidance, including our Privacy Chapters in the Departmental Manual, 383 DM 1 through 13.

The privacy rights coded into the Privacy Act are based on the Code of Fair Information Principles developed by the former Department of Health, Education and Welfare, and include:

(A) *Openness*. The public will be informed about the existence and main purpose of agency information systems.
(B) *Right of Access and Correction*. Individuals have the right to view all information collected about them, and must be able to correct or remove data that is not timely, accurate, relevant or complete.
(C) *Collection Limitation*. Collection of personal data should be collected only by lawful and fair means and, where appropriate, with the consent of the individual.
(D) *Data Quality*. Personal data should be relevant to the purposes for which collected and used, and must be accurate, complete, and timely.
(E) *Finality*. There should be limits to the use and disclosure of personal data. Data should be used only for purposes specified at the time of the collection of the information and should not be otherwise disclosed without consent.
(F) *Security*. Personal data should be protected by reasonable security safeguards against such risks as loss, unauthorized access, destruction, use modification, or disclosure.
(G) *Accountability*. Record keepers should be accountable for complying with fair information practices.

The DOI has many established procedures, policies and practices to ensure that the various elements of these fair information practices, as mandated by the Privacy Act, are carried out. These procedures and policies span the life cycle of all agency records and systems—over the planning, creation, use, modification, and retirement of such records or systems. Policy and procedures currently exist for the handling of sensitive or privacy information at these various phases, including the end of the life of such records or systems.

DOI has the responsibility to collect only the minimum privacy information needed to accomplish its mission, ensuring it is relevant and timely as appropriate for agency use. In addition, DOI must continuously review alternatives allowing reduction of privacy information collected; such consideration is part of the system of records or Privacy Impact Assessment development process at the Department. In accordance with our Departmental Security IT Policy Handbook, the Department complies with the Federal Information Security Management Act of 2002 (FISMA) and has implemented a comprehensive information security program to ensure appropriate safeguards are in place. The Department requires adherence to National Institute of Standards and Technology (NIST) controls in protection of electronic systems, and uses the Cyber Security Assessment and Management (CSAM) System to ensure that the full range of appropriate NIST controls are used throughout the Department in the certification and accreditation of systems. Additionally, the Department's compliance with the Privacy Act, the E-Government Act, OMB guidance, and other regulations and laws is designed to assure that these practices for privacy protection practices are fulfilled.

In accordance with current Departmental policy, the privacy aspects of overall agency operations are supervised at the management level by the Senior Agency Official for Privacy (SAOP), who is the Departmental Chief Information Officer (CIO). This individual works closely with the Departmental Privacy Officer, who has hands-on management and oversight of the Privacy Program, including oversight of the bureau and major office privacy programs throughout the Department. Finally, each bureau or major office of the Department has a bureau Privacy Officer who manages privacy matters such as development of system of records notices and Privacy Impact Assessments within the bureau. Such efforts are quarterly and annually reported to the OMB through regular FISMA and E-Government reporting, as well as Exhibit 300s submissions. Further, the Department's Office of Inspector General (IG) audits compliance with these requirements.

Within the Department, policy requires that all information will be retained in accordance with Records Schedules which are to be developed for all systems of information throughout the Department. Such schedules are required to be in conformity with the National Archives and Records Administration (NARA) Guidelines and the Federal Records Act. Further, it is the policy of the Department to only retain information for which it has legal authority to retain.

The following are some of the major Departmental rules and guidance documents concerning privacy program requirements:

Departmental Privacy Act Regulations at 43 CFR 2.45 – 2.79
Departmental Manual Privacy Chapters 383 DM 1-13
OCIO Directive 2006-16 on Safeguarding Personally Identifiable Information
Publication of System of Records Notices
Publication of Public Versions of Privacy Impact Assessments
Posting of Various Guidance Documents concerning the protection of PII at "DOI Privacy Guidelines and References"
IRM Bulletin 2001-004 on "Protecting Sensitive Data When Transferring Donating or Disposing of Computer Equipment

b. Rules Assessment. The ISE Privacy Officials shall implement a process for the regular assessment and review of all of the laws, Executive Orders, policies and procedures that apply to the protected information that it will make available or accessible through the ISE. The Department will also examine the existing and new internal policies and procedures regarding procedures, rules and agreements for activities related to the ISE, including rules for gathering or collecting information, permitting the correction of such information, and the dissemination of this information. Such rules will be reviewed at least annually to ensure conformity with any new legislation or guidance, new technology, or new circumstances which may generate a need for revision. These procedures will continue to be in conformity with current privacy protections under existing laws, such as the Privacy Act.

Any rules relating to the ISE will conform to the Department's existing legal provisions regarding the rights of individuals. The Senior ISE Privacy Official and Departmental

Privacy Officer, the Deputy ISE Privacy Official, are responsible for the ongoing monitoring and assessment of such rules and will work with law enforcement as needed to tailor such additional specific policies and procedures which are required for ISE-specific decision making. These ISE Privacy Officials, and the Departmental and bureau law enforcement bodies, will work collaboratively to implement the provisions of the DOI ISE Privacy Policy.

At a minimum, such policies and procedures shall address the following: The day to day responsibility of the law enforcement bodies of the Department, which include the Office of the Inspector General, BIA Law Enforcement, BLM Law Enforcement, FWS Law Enforcement, BOR Law Enforcement, NPS Law Enforcement, and Departmental Law Enforcement and Security Offices with respect to Information Sharing. Senior management in the Department will also be consulted regarding written agreements for ongoing sharing of information, such as through access to databases and standing protocols, as well as for the deployment of resources, including staffing and funding for such activities. Law enforcement staff will receive specific training in the ISE requirements as soon as possible upon or before being so designated. Such training will include coverage of this policy and explain the parameters of privacy protection during the decision processes of law enforcement compliance with the ISE. Further, the ISE Privacy Officials will have oversight of such compliance.

The ISE Privacy Officials will also be responsible for updating and reviewing any rules and written agreements concerning sharing in use by Departmental personnel, including law enforcement personnel, to ensure the ongoing protection of privacy and civil rights while facilitating the necessary sharing under the ISE regarding terrorist or illegal activity.

c. Changes. Whenever there is an identification of an issue that poses a significant risk to information privacy rights or other legal protections, the Departmental ISE Privacy Officials will promptly address the matter. Whenever these officials identify an internal policy that significantly impedes the sharing of terrorism, homeland security, or law enforcement information in a manner that does not appear to be required by applicable laws or to protect information privacy rights or provide other legal protections, they shall review the advisability of maintaining such restriction. Finally, whenever the DOI ISE Privacy Officials identify a restriction on sharing protected information other than one imposed by internal agency policy that significantly impedes the sharing of information in a manner that does not appear to be required to protect information privacy rights or provide other legal protections, they shall review such restriction with the ISE Privacy Guidelines Committee for further action as appropriate. If an appropriate internal resolution cannot be developed, the DOI ISE Privacy Officials may bring such restriction to the attention of the Attorney General and the Director of National Intelligence who, in accordance with the ISE Guidelines, shall review any such restriction and jointly submit any recommendations for changes to the Assistant to the President for Homeland Security and Counterterrorism, Assistant to the President for Homeland Security and Counterterrorism, Assistant to the President for National Security Affairs, and the Director of the Office of Management and Budget for further review.

Purpose Specification.

The purpose of this policy is to protect the privacy and civil rights interests of citizens, permanent lawful residents, and others in mixed systems as required by the Constitution, statutes, regulations and guidance while providing for appropriate sharing of terrorism, homeland security, or law enforcement information within the ISE. The Department has written guidance in place on what privacy information may be collected. Such guidance is found in the Privacy Act regulations, Departmental Manual Chapters, OCIO Memoranda, and other Departmental Privacy guidance, all of which may be found on the DOI web site at http://www.doi.gov/ocio/privacy. Such guidance also clearly states that the purposes for which information is intended to be used in any applicable system of records or Privacy Impact Assessment must be appropriate for the business case needs of the program office managing the system, and that any routine uses for sharing of such information must be compatible with the original purposes for which the system was created.

Identification of Protected Information to be Shared through the ISE.

Identification and Prior Review. Departmental, bureau, and office law enforcement personnel will review all law enforcement holdings that contain protected information and information about nonresident aliens contained in mixed systems. It is the responsibility of law enforcement officers to ensure that all collection and sharing of information is in full compliance with policy and subject to oversight by the ISE Privacy Officials.

Notice Mechanisms. In order for ISE participants who receive information to handle protected information and information about nonresident aliens contained in mixed systems in accordance with applicable legal requirements, affected bureaus and offices will establish notice mechanisms for communicating information regarding the nature of the information made available to the ISE participants. This notice will, to the extent feasible, permit ISE participants to determine whether the information pertains to a U.S. citizen, lawful permanent resident, or to another party within a mixed system; is subject to specific information privacy requirements; and has any limitations on reliability or accuracy.

Data Quality.

Accuracy, Notice of Errors, and Procedures. The DOI strives to use and share only 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 has reasonable safeguards to protect the integrity of the data. The Department will take a number of steps to ensure that the data used are of the highest quality, identified errors will be properly followed up, and that procedures are in place to provide information that is reliable and accurate. Therefore:

- Upon receiving information within the ISE that DOI determines may be inaccurate, DOI will ensure that a written correction is made and that other appropriate officials are informed;

- 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 DOI 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;
- DOI will follow existing redress mechanisms whereby individuals may request correction of their data from bureau or Departmental Privacy Officers and will ensure that such mechanisms apply also to ISE sharing situations;
- When merging protected information about an individual from two or more sources, the DOI will take appropriate steps to ensure that the information is about the same individual and document this effort wherever undertaken;
- DOI will investigate in a timely manner alleged errors and deficiencies and correct, delete, or refrain from using protected information found to be erroneous or deficient; and
- DOI will retain protected information only as long as it is relevant and timely for appropriate use by the agency and will update, delete, or refrain from using protected information that is outdated or otherwise irrelevant for such use.

Additionally, the DOI ISE Privacy Officials will ensure that data quality reviews occur at systems development, and with routine monitoring, to prevent inaccurate data to the extent feasible.

Data Security.

Under Departmental regulation and guidance, privacy information—in whatever media—must be kept in a locked, secure environment with access only granted to those who have a need to use the information and who have been properly trained and are carefully supervised. Under its security responsibilities for electronic data as laid out in the Departmental IT Security Policy Handbook, system owners and managers of electronic systems must follow current NIST controls to assure that the information is continuously available, confidential, and maintains its integrity for accuracy and completeness. Such requirements focus on various areas including proper screening of staff, training, security configuration, hardware and software protections, authorizations, passwords and authentication, roles and levels of access, testing of systems and quality control, certification and accreditation of systems, etc. For systems containing privacy information, some of these NIST controls are directed toward privacy issues. The review process for all electronic systems is conducted at two levels within the Department: the internal program level, followed by an independent review outside of the program office. Such efforts are documented for all DOI electronic systems in the DOJ CSAM database. When systems contain privacy information, they are subject to additional requirements, including review by bureau privacy officers to ensure the adequacy of protection as

described in related documentation (Privacy Impact Assessments, system of records notices, where applicable, etc.).

All ISE activities will follow procedures that ensure, at a minimum, these levels of procedural safeguarding of data quality.

Accountability, Enforcement and Audit.

The DOI ISE Privacy Officials (see Governance section, below) shall serve as the primary providers of oversight for the privacy protection aspects of the ISE implementation at the Department. They shall be responsible for reporting to senior management on the status of any privacy aspects of ISE implementation and activities at the Department. They will continue to provide guidance to the bureaus and offices within the Department for privacy protection and will issue any needed guidance and procedures for the ISE. Their activities are also continually subject to the monitoring and oversight of the DOI Office of Inspector General.

The Department is committed to accountability for the acceptable use of protected information and information about nonresident aliens contained in mixed systems. DOI demonstrates this accountability through a variety of mechanisms, including:

- Provisions of transparency about its participation in ISE through various notice mechanisms including the publication of this policy, system of records notices, and Privacy Impact Assessments on its website;
- Providing training to all employees, contractors and volunteers in privacy, records management, and IT security awareness before granting access to agency systems, and annually thereafter;
- In coordination with OLES and other law enforcement officials, assisting—if needed—in providing specialized, role-based training to those persons authorized to handle protected information and information about nonresident aliens contained in mixed systems; and
- Taking appropriate action when violations of its privacy policies are discovered. Individuals who fail to implement safeguards will be held accountable through disciplinary or corrective actions, and willful violations of the Privacy Act call for criminal penalties for non-compliance including fines of up to $5,000 per violation.

To ensure implementation of the DOI ISE Privacy Policy, the ISE Privacy Officials, in conjunction with the bureau Privacy Officers, will review at least annually any DOI ISE policies and practices, including those relating to the collection, access, use, disclosure, and destruction of covered information, to ensure such practices comply with this policy. In addition, the DOI ISE Privacy Officials will develop specific auditing and monitoring procedures as needed to ensure proper fulfillment of and compliance with this policy.

Redress.

To seek redress for privacy issues concerning the ISE, an individual may follow a number of existing remediation avenues. The primary means of redress is through adherence to the Privacy Act procedures which permit citizens, permanent resident aliens, and those persons in mixed Privacy Act systems of records to access and seek to correct their information. Any individuals, regardless of personal status, may seek notification of and access to any record on themselves maintained by the agency, with the exception of exempted records, in accordance with 43 CFR 2.79. Under Section 2.75, an individual may seek correction or completion of such personal privacy information, as appropriate. Additionally, individuals who believe that their information may have been inappropriately shared within the ISE by the DOI, or who have any other privacy complaints concerning DOI programs or activities, may submit such complaints to the Departmental Privacy Officer whose contact email is located at: http://www.doi.gov/ocio/privacy/doi_privacy_act_officers.htm.

Specifically regarding the ISE, anyone seeking redress may contact an ISE Privacy Official and state the nature of the issue in writing. As noted in the Data Quality section, appropriate follow-up action will then be determined and implemented.

Also, individuals desiring access to agency information gathered about them, whether in privacy systems of records, or in other records, may submit a request to the appropriate Freedom of Information Act Officer for the bureau most closely related to the system or source of information. In addition, inquiries about information, as well as corrections for any information, may be requested through the bureau Privacy Officers or through the Departmental Privacy Officer. The ISE Privacy Officials will review applicable policies and rules within these individual bureaus and offices concerning the ISE redress, and ensure and monitor compliance. The ISE Privacy Officials will maintain a record of all such specific ISE redress requests.

Execution, Training, and Technology.

a. Execution. The ISE Privacy Officials are responsible for implementing the DOI ISE Privacy Policy throughout the Department. They will ensure that the policy is carried out through appropriate procedures, rules, and compliance.

b. Training. In order for this policy to be properly implemented, all personnel involved in accessing or using information sharing systems within the ISE must receive specific ISE training as soon as practicable after they are identified. ISE Privacy Officials and senior law enforcement will collaborate to determine the specifics and nature of the training. All bureau and office supervisors, program leads, law enforcement personnel, and managers including senior management are encouraged to take the half-hour online ISE Core Awareness Training Computer-Based Training (CBT) on the ISE website at www.ise.gov. All employees, contractors and volunteers will be responsible for abiding by the requirements of this Departmental ISE Privacy Policy and all other policies governing the use of PII and shall be held accountable.

c. *Technology*. The Department regularly considers technology enhancements to protect privacy within electronic systems through its Privacy Impact Assessment review process. Many measures are already in place and regularly used, including stringent, NIST-compliant requirements for user IDs and passwords; authentication; minimal collection of PII to accomplish agency missions; use of firewalls; encryption; levels of access based on the need to know and use; universal use of NIST controls for certified and accredited systems; system logs; auditing; key logging; and flagging on transmission of certain sensitive information, etc. DOI will vigorously continue to explore avenues of privacy protection. Any feasible technological enhancements to privacy protection will be acquired and utilized.

Awareness.

The Department will post this ISE policy on its public website. The Departmental Privacy Officer may be contacted for particular questions regarding the policy.

Additionally, the Department has the responsibility to ensure transparency in its information handling. This is accomplished by a number of DOI policies and practices including:

(A) Requiring systems of records notices be published in the Federal Register for paper or electronic systems which are retrieved by personal identifiers;
(B) Requiring Privacy Impact Assessments for all electronic systems that contain personal privacy information. Note that the Department requires these whether the information pertains to the public or to employees, going beyond the minimum requirements of the E-Government Act;
(C) Posting links of the Departmental website to its system of records notices, Privacy Impact Assessments, and its various privacy policies and procedures;
(D) Providing contact information for Departmental and bureau Privacy and FOIA Officers; and
(E) Providing online access to the Departmental Privacy Act regulations, as well as the Departmental Manual Chapters for Privacy.

Non-Federal Entities.

To the extent consistent with applicable Federal laws and guidance governing the protection of information privacy and other legal rights, the DOI 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.

Governance.

a. ISE Privacy Officials. The Departmental Chief Information Officer (CIO) shall be designated as the Senior DOI ISE Privacy Official responsible for implementing and

managing Departmental policy and compliance concerning the Information Sharing Environment. This person will work closely with the Departmental Privacy Officer who will serve as the Deputy DOI ISE Privacy Official and will provide additional hands-on responsibility for implementation of this policy. These ISE Privacy Officials will consult with the Deputy Assistant Secretary – Law Enforcement and Security and the senior Departmental management team, all of whom will assist to the fullest extent possible in carrying out the policy. The DOI ISE Privacy Officials shall also be responsible for ensuring that the Department's ISE Policy is disseminated to all bureaus and offices within the Department, with the directive that it be shared with all employees including contractors and volunteers. The Senior ISE Privacy Official may also convene a standing task force consisting of both law enforcement and senior Department officials who shall serve to assist in policy and procedural management of Departmental ISE initiatives. The DOI Privacy Officer, also serving as a DOI ISE Privacy Official, shall be a permanent member of any such task force.

b. ISE Privacy Guidelines Committee. The Department of the Interior will abide by the ISE Guidelines as participants in the ISE. Such compliance includes future modifications to such Guidelines, or other guidance as issued by the ISE governance process. In addition, DOI ISE Privacy Officials will participate in the Interagency Privacy Policy Committee meetings and will otherwise act to promote the effective functioning of the ISE.

c. Privacy and Civil Liberties Oversight Board. The Department will consult with the Privacy and Civil Liberties Oversight Board (PCLOB) as appropriate regarding its development and use of the ISE. The Department will act collaboratively with the PCLOB.

d. ISE Privacy Protection Policy. This DOI ISE Privacy Policy is developed in conformity with the ISE requirement for implementation of the ISE Guidelines.

General Provisions.

a. Definitions.

Agency. The term "agency" has the meaning set forth for the term "executive agency" in section 105 of title 5, United States Code, but includes the Postal Rate Commission and the United States Postal Service and excludes the Government Accountability Office.

Agency Sensitive Information. Agency sensitive information, while not specifically protected information under the IRTPA, is nevertheless to be protected because of other laws such as the Freedom of Information Act. Agency sensitive information refers to information the agency holds that under law should not be released to the public but for reasons other than personal privacy or private sector proprietary business information, both of which are protected under the ISE Guidelines. Several examples of agency sensitive information, which the Department will also protect, include specifics of law enforcement information, Government business proprietary information, critical infrastructure

information, attorney work product information, and any information which could enable the circumvention of a law or the commission of a crime.

Homeland Security Information. Homeland Security Information, as derived from the Homeland Security Act of 2002,[3] is defined as any information possessed by a state, local, tribal, or Federal agency that:

(A) Relates to a threat of terrorist activity;
(B) Relates to the ability to prevent, interdict, or disrupt terrorist activity;
(C) Would improve the identification or investigation of a suspected terrorist or terrorist organization; or
(D) Would improve the response to a terrorist act.

Law Enforcement Information. Law Enforcement Information is defined as 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:
(1) Information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation;
(2) Assessment of or response to criminal threats and vulnerabilities;
(3) The existence, organization, capabilities, plans, intention, vulnerabilities, means, method, 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;
(4) The existence, identification, detection, prevention, interdiction, disruption of, or response to criminal acts and violations of the law;
(5) Identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and
(6) Victim/witness assistance.

Privacy information. Privacy information is personally identifiable information, 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. Such information includes both the standard information regarding the identification of an individual, such as social security number, date of birth, full name and personal address, and additional information about personal attributes of the individual, including biometric data, non-work affiliations and beliefs, and financial, medical, or family information.

Protected information. Protected information is information about U.S. citizens and permanent lawful residents (and others where their status is not easily determined) that is subject to privacy protection or to other legal protections under the Constitution or laws of the United States. Such legal protections include civil rights to not be discriminated against because of certain categories or conditions (race, age, etc.). Protected information

[3] *6 U.S.C. 482(f)(1).*

under the ISE Privacy Guidelines also includes other information such as business proprietary information, especially where the business entity is primarily controlled or owned by U.S. citizens or U.S. permanent legal aliens.

Terrorism information. Under the IRTPA, the term "terrorism information" means all information—whether collected, produced, or distributed by intelligence, law enforcement, military, or homeland security—or other activities relating to:

(A) 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;
(B) threats posed by such groups or individuals to the United States, United States persons, United States interests, or to those of other nations;
(C) communications of or by such groups or individuals; or
(D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Terrorist information also includes information about weapons of mass destruction, homeland security information, and law enforcement information relating to terrorism or the security of our homeland, including intelligence information.

Weapons of Mass Destruction Information. Weapons of Mass Destruction Information is defined in IRTPA Section 1016 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 terrorist organization against the United States, including information about the location of a stockpile of nuclear materials that could be exploited for use in such a weapon that could be used by a terrorist or terrorist organization against the United States.

(B) The treatment of information as "protected information" under this Policy does not by itself establish that the individual or entity to which such information pertains does in fact have information privacy or other legal rights with respect to such information.

(C) All personnel at the Department of the Interior, including all levels of Management shall, to the extent permitted by law, provide the cooperation, assistance, and information necessary for the implementation of the ISE Privacy Policy at the Department.

(D) This ISE Privacy Policy:

(i) is to be implemented in a manner consistent with all applicable laws and Executive Orders, including Federal laws protecting the information privacy rights and other legal rights of Americans, of

permanent resident aliens, and of others when their information is in mixed systems;

(ii) shall be implemented in a manner consistent with the statutory authority of the Secretary of the Interior, Deputy Secretary, Assistant Secretaries, and other Managerial personnel of the Department;

(iii) shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budget, administrative, and legislative proposals; and

(iv) is intended only to improve the internal management of the Federal Government and is not intended to—and does not—create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, the Department of the Interior, any of its components, or any of its personnel.

APPENDIX A

Glossary of Acronyms

Acronym	Definition
CIO	Department of the Interior's Chief Information Officer
CSAM	Cyber Security Assessment and Management System
DHS	Department of Homeland Security
DOI	Department of the Interior
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
FISMA	Federal Information Security Management Act of 2002
HSIN	Homeland Security Information Network
IG	DOI's Inspector General
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISE	Information Sharing Environment
IT	Information Technology
JTTF	Joint Terrorism Task Force (JTTF)
LEO	FBI's Law Enforcement Online
LinX	Naval Criminal Investigative Service's Law Enforcement Information Exchange
NARA	National Archives and Records Administration
NCTC	National Counterterrorism Agency's National Counterterrorism Center
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PCLOB	Privacy and Civil Liberties Oversight Board
PII	Personally Identifiable Information
SAOP	Senior Agency Official for Privacy
TSC	Terrorist Screening Center
RDex	FBI's Regional Data Exchange
RISS	Regional Information Sharing System

APPENDIX B

Version Control Record

Version	Date	Description of Revision/Update	Distribution
1.0.0		Initial Release	All Employees, Contractors, Volunteers and the Public

Approved:

1-26-2010

Sanjeev Bhagowalia
Chief Information Officer
Department of the Interior

Date