Information Sharing Environment Privacy Guidelines

Frequently Asked Questions
Version 2.1
Last updated: March 20, 2009

This document will be updated and expanded—please check back frequently.

Definitions

General Questions About the Information Sharing Environment

General Questions About the ISE Privacy Guidelines

Federal Agencies

State, Local, and Tribal (SLT) Agencies

- How does an SLT agency determine what protected information will be shared through the ISE?
- Is our SLT agency-approved privacy policy sufficient for ISE Privacy Guidelines compliance?
- Does compliance with 28 CFR Part 23 enable us to participate in the ISE?
- Does participation in a statewide fusion center meet the requirements to participate in the ISE?
- Will SLT agencies that currently share information with federal agencies be able to continue sharing information in light of the ISE Privacy Guidelines?

Other Nonfederal Entities

- Apart from state, local, and tribal governments, what other nonfederal entities will be participating in the ISE?
- Are private sector entities involved in the planning of the ISE?
- What are the guidelines for sharing with private sector entities?
- What are the guidelines for sharing with foreign partners?
- Do the ISE Privacy Guidelines cover personally identifiable information about non-U.S. persons that is made available by foreign partners?

Definitions

Information Sharing Environment (ISE)—The Information Sharing Environment (ISE) is an approach to the sharing of information related to terrorism that is being implemented through a combination of policies, procedures, and technologies designed to facilitate the sharing of critical information by all relevant entities. The ISE serves the dual imperatives of enhanced information sharing to combat terrorism and protecting the information privacy and other legal rights of Americans in the course of increased information access and collaboration. The ISE is being developed by bringing together, aligning, and building upon existing information sharing policies and business processes and technologies (systems), and by promoting a culture of information sharing through greater collaboration. It is being developed pursuant to Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007 (IRTPA) and Executive Order 13388, titled "Further Strengthening the Sharing of Terrorism Information to Protect Americans."

IRTPA—IRTPA stands for the Intelligence Reform and Terrorism Prevention Act of 2004, as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007, Public

Law 108-458, as amended by Public Law 110-53. The ISE is covered by Section 1016 of IRTPA, codified at 6 USC 485.

ISE Privacy Official—The ISE Privacy Official is the official responsible for directly overseeing the agency's implementation of and compliance with the ISE Privacy Guidelines. The agency's senior official with overall agencywide responsibility for information privacy issues (as designated by statute or Executive Order or as otherwise identified in response to the Office of Management and Budget (OMB) Memorandum M-05-08 dated February 11, 2005) will serve as the ISE Privacy Official, unless the head of the agency determines that a different official would be better situated to perform this role. See Section 12(a) of the ISE Privacy Guidelines.

ISE Privacy Guidelines Committee—The ISE Privacy Guidelines Committee is a standing committee established by the PM-ISE composed of each Information Sharing Council agency's ISE Privacy Official. The Committee provides ongoing guidance on the implementation of the ISE Privacy Guidelines, so that, among other things, agencies follow consistent interpretations of applicable legal requirements, avoid duplication of effort, share best practices, and have a forum for resolving issues on an interagency basis. See Section 12(b) of the ISE Privacy Guidelines.

PM-ISE—PM-ISE stands for the Program Manager for the Information Sharing Environment. This position was established by IRTPA Section 1016(f) and is further described within this document.

Protected Information—Protected Information is information about U.S. citizens and lawful 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." See Section 1 of the ISE Privacy Guidelines. 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. And for the 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 lawful permanent residents.

Terrorism Information—Terrorism Information is defined in IRTPA Section 1016 (codified at 6 USC 485) 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; or

- Groups of individuals reasonably believed to be assisting or associated with such groups or individuals.

The definition 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.

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:

- Related to terrorism or the security of our homeland, and
- Relevant to a law enforcement mission, including but not limited to:
    - Information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counter terrorism investigation;
    - An assessment of or response to criminal threats and vulnerabilities;
    - 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;
    - The existence, identification, detection, prevention, interdiction, or disruption of, or response to, criminal acts and violations of the law;
    - Identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and
    - Victim/witness assistance.

Weapons of Mass Destruction Information—Weapons of Mass Destruction Information is defined in IRTPA Section 1016 (codified at 6 USC 485) 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.

Civil Rights—The term *civil rights* refers to those rights and privileges of citizenship and equal protection that the state is constitutionally bound to guarantee all citizens regardless of race, religion, sex, or other characteristics unrelated to the worth of the individual. Protection of civil rights imposes an affirmative obligation upon government to promote equal protection under the law. These civil rights to personal liberty are guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress. Generally, the term *civil rights* involves positive (or affirmative) government action to protect against infringement.

Civil Liberties—The term *civil liberties* refers to fundamental individual rights such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the

government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights—the first ten Amendments—to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference.

General Questions About the Information Sharing Environment

What is the Information Sharing Environment (ISE)?

The Information Sharing Environment (ISE) is an approach to the sharing of information related to terrorism that is being implemented through a combination of policies, procedures, and technologies designed to facilitate the sharing of critical information by all relevant entities. The ISE serves the dual imperatives of enhanced information sharing to combat terrorism and protecting the information privacy and other legal rights of Americans in the course of increased information access and collaboration. The ISE is being developed by bringing together, aligning, and building upon existing information sharing policies and business processes and technologies (systems), and by promoting a culture of information sharing through greater collaboration. It is being developed pursuant to Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007 (IRTPA) and Executive Order 13388, titled "Further Strengthening the Sharing of Terrorism Information to Protect Americans."

What is the purpose of establishing the ISE?

The ISE will create the conditions by which information can be accessed across agency and jurisdictional boundaries and between the federal government and its state, local, and tribal agency, private sector, and foreign partners in a timely, efficient, and frictionless manner while protecting the information privacy and other legal rights of Americans.

Historically, the sharing of terrorism-related information has taken place within multiple sharing environments and within individual communities of interest, including the intelligence, law enforcement, defense, homeland security, and foreign affairs communities. Each of these communities of interest developed its own legal and operational information sharing framework to accomplish specific mission requirements. As a result, the information sharing environment that existed on 9/11 was not as integrated, interconnected, or robust as the nation required. The purpose of the ISE is to facilitate the sharing and integration of terrorism-related information between and among the agencies and entities comprising the traditional information sharing environments and communities of interest without diminishing individuals' privacy rights or civil liberties.

Is the ISE a single database, system, or repository?

No. The ISE will not be a massive new information system. Rather, it will provide a new way to access, use, and transmit terrorism-related information through existing systems of the participating agencies. While the ISE will use technology to the maximum extent possible to enhance information sharing, it will not result in the construction of a single interconnected computer system or repository containing all terrorism information.

What information will be shared through the ISE?

The ISE will facilitate the sharing of terrorism information (which includes weapons of mass destruction information), homeland security information, and law enforcement information

(collectively referred to as terrorism-related information because, as defined, each of these types of information has a terrorism nexus).

What is the position of Program Manager (PM) for the ISE (PM-ISE), and what are its duties?

IRTPA Section 1016 requires the President to designate an individual to serve as the Program Manager (PM) for the Information Sharing Environment (PM-ISE). The PM-ISE's duties include:

- Planning, overseeing the implementation of, and managing the ISE.
- Assisting in the development of policies to foster the development and proper operation of the ISE.
- Issuing governmentwide procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE.
- Identifying and resolving information sharing disputes between federal departments, agencies, and components.
- Assisting, monitoring, and assessing the implementation of the ISE by federal departments and agencies to ensure adequate progress, technological consistency, and policy compliance; and regularly reporting the findings to the U.S. Congress.

The PM-ISE will build upon current information sharing efforts across the U.S. government, facilitating change and acting as a catalyst for improving terrorism-related information sharing among ISE communities by working with them to remove barriers and improve information access.

Who is the PM-ISE?

On March 15, 2006, the President designated Ambassador Thomas E. McNamara to serve as the PM-ISE. Ambassador McNamara possesses extensive background in national security matters, political-military affairs, counterterrorism, and counternarcotics.

The Ambassador is a career diplomat whose postings overseas include Colombia, Russia, Congo, and France. In the 1980s, he was a Deputy Assistant Secretary of State, National Security Council (NSC) Director, and Ambassador to Colombia. On his return from Colombia in 1991, he served President George H. W. Bush as Special Assistant for National Security Affairs before returning to the State Department as Ambassador-at-Large for Counter Terrorism and Assistant Secretary of State for Political-Military Affairs. In 1998, he was appointed the Special Negotiator for Panama. Upon his retirement from government service in 1998, he became President and CEO of the Americas Society and the Council of the Americas in New York. Following the attacks of September 11, 2001, Ambassador McNamara was asked to return to the State Department and served as the Senior Advisor for Counter Terrorism and Homeland Security to the Secretary and Deputy Secretary until 2004. Most recently, in addition to serving as the PM-ISE, the Ambassador has been an adjunct professor in the Elliott School of International Affairs at The George Washington University in Washington, DC.

What government agency houses the Office of the PM-ISE?

In June 2005, the President directed that the Office of the PM-ISE be located in the Office of the Director of National Intelligence (ODNI).

What is the ISE Implementation Plan (ISE IP)?

The *Information Sharing Environment* (ISE) *Implementation Plan* (ISE IP) (November 2006) is a three-year plan that implements the 11 requirements set forth in IRTPA Section 1016 (e) and by the President in his December 2005 Memorandum titled "Guidelines and Requirements in Support of the Information Sharing Environment." The ISE IP describes the actions that the federal government intends to carry out over a three-year period in coordination with state, local, and tribal agencies; private sector entities; and foreign partners.

A copy of the ISE Implementation Plan can be found at www.ise.gov. Chapter 9 addresses protections for information privacy and civil liberties in implementing the ISE.

What is the governance structure for the ISE?

The ISE has a three-part governance structure:

1. Program Manager (PM) for the ISE (PM-ISE)
2. Information Sharing Council (ISC)
3. Information Sharing Policy Coordination Committee (ISPCC)

The function of the Program Manager is described in a separate frequently asked question.

The Information Sharing Council is an interagency forum, established by IRTPA Section 1016 and Executive Order 13388, to advise the President and the Program Manager and to provide for coordination among the Federal agencies participating in the ISE. Chaired by the PM, the ISC is a means for the PM to assess progress among ISE communities. The ISC has established two subcommittees to address local, state, and tribal agency and private sector issues. These subcommittees are co-chaired by the U.S. Department of Homeland Security (DHS) and the U.S. Department of Justice (DOJ).

The Information Sharing Policy Coordination Committee was established in June 2006 by the President to address major information sharing policy issues, including the resolution of PM-raised issues, and to provide policy analysis and recommendations for consideration by the more senior committees of the Homeland Security Council (HSC) and National Security Council (NSC). The Program Manager is also a member of ISPCC.

The White House Privacy and Civil Liberties Oversight Board was established to provide advice and counsel on the development and implementation of policy to the President or to the head of any executive department or agency. IRTPA Section 1016 required consultation with the PCLOB in protecting the information privacy rights, civil rights, and other legal rights of Americans with regard to ISE development and use. The PM and ISC worked closely with the PCLOB to ensure the protection of privacy and civil liberties throughout initial ISE development and management. This Board's statutory term expired on January 30, 2008.

Recently, a restructured Privacy and Civil Liberties Oversight Board (PCLOB) was established by the Implementing Recommendations of the 9/11 Commission Act of 2007 (IRTPA, Section 1061) to help ensure the protection of privacy and civil liberties and ensure that liberty concerns are appropriately considered in efforts to protect the nation against terrorism.

Where can I find more information about the ISE?

More information can be found at www.ise.gov.

General Questions about the ISE Privacy Guidelines

What are the ISE Privacy Guidelines?

In his December 16, 2005, Memorandum to the Heads of Executive Departments and Agencies on "*Guidelines and Requirements in Support of the Information Sharing Environment*," the President directed that the Attorney General and the Director of National Intelligence:

- Conduct a review of current executive department and agency information sharing policies and procedures regarding the protection of information privacy and other legal rights of Americans; and
- Develop Guidelines designed to be implemented by executive departments and agencies to ensure that the information privacy and other legal rights of Americans are protected in the development and use of the ISE, including the acquisition, access, use, and storage of personally identifiable information.

In November 2006, the President approved and the Program Manager issued the *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* (ISE Privacy Guidelines). The Guidelines present principles for federal departments and agencies to follow to ensure that the information privacy rights and other legal rights of Americans are protected as personally identifiable terrorism-related information is acquired, accessed, used, and stored in the ISE. Simply stated, the ISE Privacy Guidelines establish a framework for sharing such information in the ISE in a manner that protects privacy and other legal rights. The framework balances the dual imperatives of sharing information and protecting privacy by establishing uniform procedures to implement required protections, in particular legal and mission environments. In addition, the framework establishes an ISE privacy governance structure for deconfliction, compliance, and continuous development of privacy guidance.

To whom do the ISE Privacy Guidelines apply?

The ISE Privacy Guidelines apply by their terms to federal agencies in their development and use of the ISE. The Guidelines require each agency to develop a written ISE privacy protection policy that sets forth the mechanisms for implementing the Guidelines. The Guidelines may serve as a model for other entities that enter the ISE arena as terrorism-related information sharing partners.

What information is covered by the ISE Privacy Guidelines?

The ISE Privacy Guidelines apply to protected information.

Apart from privacy, what other legal rights are embraced by the concept of "protected information?"

Information in the ISE may enjoy legal protections that are not strictly related to privacy. For example, information relating to the exercise of civil liberties protected by the Bill of Rights may be subject to constitutional protections. In addition, civil rights laws establish protections for individuals that may need to be considered as information is shared in the ISE. For the Intelligence Community, information about U.S. corporations or associations may be subject to protection under Executive Order 12333. Finally, the term "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 protected. However, it is anticipated that, in most cases, protections will focus on the privacy of personally identifiable information about U.S. citizens and lawful permanent residents.

What might be the civil rights and civil liberties considerations that apply in the ISE?

As an ISE participant, your agency's information collection, use, and sharing activities may implicate individuals' civil rights and civil liberties (CR/CL). Our freedoms are essential to our way of life as Americans. As agency staff go about their duties, they should keep in mind the legal and cultural importance of civil liberties in American life. When a question arises, seek guidance from existing policies and procedures and, if a topic is not covered, raise the issue with a supervisor or agency legal counsel.

Generally the term "civil rights" refers to the duty of government or certain private actors such as businesses or landlords to respect and protect individual rights. In contrast, "civil liberties" typically involve restrictions on government that have the effect of respecting individuals' freedom to do certain things. See the **Definitions** of terms for detailed definitions of these terms.

What CR/CL issues might arise for ISE participants?

The most likely areas where such issues might arise are:

- Acquisition of information—e.g., information from an illegal search, or otherwise collected in an illegal or improper manner;
- Agency retention or use of information for unlawful or improper purposes—e.g., collection of First Amendment information that is not linked to criminal or national security activity;
- Dissemination of information through the ISE—If information acquired in the ISE is not properly vetted (reviewed for accuracy, completeness, timeliness, and relevancy) or protected and its proper use controlled, then sharing this information with ISE partners may affect the CR/CLs of individuals identified in that information, or later subjected to enforcement action based on the information. A good example is information that is later determined to be inaccurate, incomplete, untimely, or irrelevant. The wider the dissemination of this information, the greater the potential harm or disruption to the life of the affected individual—for instance, if that information is used in obtaining a warrant to search an individual's home or to arrest the individual.

With the national focus on the rapid sharing of terrorism-related information, an area of special vulnerability to CR/CL concerns is the information collected on individuals or groups associating with or assisting suspected terrorists or terrorist organizations.

Other areas of significant CR/CL concern include information collected based solely upon an individual's race, religion, ethnicity, or national origin; First Amendment issues; Fourth Amendment issues; and due process considerations. These issues are addressed in the next four FAQs, and detailed information on these and other CR/CL issues of concern to ISE participants is provided in the *Civil Rights and Civil Liberties Protections* "Key Issues Guidance" located on the ISE Privacy Protections page of the PM-ISE Web site at www.ise.gov.

What CR/CL issues might arise in the ISE with regard to information collected based solely on an individual's race, religion, ethnicity, or national origin?

Civil rights protections may need to be considered as intelligence and investigative information is shared in the ISE. An example in the ISE context is the sharing of information that was collected based *solely* upon an individual's race, religion, ethnicity, or national origin. Problems can be avoided by developing policies and procedures that ensure that information is not collected *solely* on this basis (e.g., by ensuring that there is a valid mission purpose in the collection). If this type of information has *already* been collected, sound policies and procedures will ensure that this type of information is tagged and is not shared with other agencies in the

ISE. Note: information regarding an individual's race or ethnicity may always be collected when it is a fact associated with identification of the individual or the individual's involvement in a crime or suspicious activities—for example, where the physical description of a bank robbery suspect includes mention of his apparent race or ethnicity. The use of race or ethnicity is subject to heightened scrutiny where it is used as a factor in law enforcement decision-making, and where actions are predicated on the assumption that individuals of a particular race or ethnicity are more likely to be involved in criminal activity. Reliance on stereotypes is always forbidden.

What CR/CL issues might arise in the ISE with regard to First Amendment-related issues?[1]

Although these issues usually arise in direct contact situations, sharing of certain types of information may raise First Amendment concerns unless an agency can show that the information was collected for legitimate law enforcement or national security interests. Examples include:

- The sharing of identifying information on anti-war protestors at a lawful rally could raise concerns.
- Collecting and sharing the membership lists of religious or political organizations where that information is exposed to the public and results in regulatory restrictions or public derision such that the group is harmed (e.g., a drop in membership).
- Use of information from video recordings of a public meeting.

If the material was collected for a legitimate law enforcement or national security purpose, additional civil liberties concerns may arise if an individual is misidentified as being associated with a terrorist or terrorist group and the information is used to his or her detriment. Agency policies should address issues such as (1) whether information will include notice of known limitations related to the collection, and (2) how confirmed misidentifications will be purged from the system.

What CR/CL issues might arise in the ISE with regard to Fourth Amendment-related issues?

Concerns here arise when an agency shares materially inaccurate or misleading information that results in the seizure of the misidentified individual or search of his or her property. If the information was initially acquired in violation of the individual's Fourth Amendment rights, then a possible later order of expungement could apply to the ISE. An expungement order may result from a court suppression hearing or an agency complaint process. These concerns can be addressed through robust data quality measures and notice to information sharing partners.

What CR/CL issues might arise in the ISE with regard to Fifth and Fourteenth Amendments-related issues?

Due process considerations may arise where erroneous information about an individual is shared and leads to the denial of the individual's entitlements, benefits, status, privileges, or other rights granted by statute. *For example*, a background check that relies upon this erroneous information results in the individual being denied a job. If the individual was not given the opportunity to challenge the facts underlying the adverse action, this may raise due process concerns.

[1] The First Amendment prohibits Congress from passing laws that prohibit the free exercise of religion, or abridge freedom of speech, freedom of the press, the right of peaceful assembly or the right to petition the government for redress of grievances. The courts have extended this to include official acts of government officials. Absent a valid law enforcement or mission-related purpose, any government act infringing on these freedoms is prohibited.

Do the ISE Privacy Guidelines override existing laws, such as the Privacy Act?

No. The ISE Privacy Guidelines do not and cannot override existing laws. To the contrary, they require compliance with applicable laws.

How do the ISE Privacy Guidelines protect privacy and other legal rights?

The ISE Privacy Guidelines build on a set of core principles that executive agencies and departments will follow. These principles require specific, uniform action across these entities and reflect basic privacy protections and best practices, requiring agencies to (among other things) identify any protected information to be shared; enable other agencies to determine the nature of the information (e.g., whether it contains information about U.S. persons); assess and document applicable legal and policy rules and restrictions; put in place notice and accountability, enforcement, and audit mechanisms; implement data quality and data security measures; provide redress, as appropriate; and identify an ISE Privacy Official with overall agencywide responsibility for information privacy issues and who will directly oversee the agency's implementation of and compliance with the ISE Privacy Guidelines.

What is the legal basis for the ISE Privacy Guidelines?

Section 1016(d) of the IRTPA calls for the issuance of guidelines to protect privacy and civil liberties in the development and use of the Information Sharing Environment (ISE). Section 1 of Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," provides that "[t]o the maximum extent consistent with applicable law, agencies shall…give the highest priority to…the interchange of terrorism information among agencies…[and shall] protect the freedom, information privacy, and other legal rights of Americans in the conduct of [such] activities…." The Guidelines implement the requirements under the IRTPA and Executive Order 13388 to protect information privacy rights and provide other legal protections to Americans in the development and use of the ISE.

What is the process for achieving compliance with the ISE Privacy Guidelines?

Because the authorities, policies, and missions of federal departments and agencies differ, the ISE Privacy Guidelines prescribe a process, rather than an end-state, with which each federal ISE participant must comply. This approach requires each department and agency, as bounded by the laws/policies/regulations applicable to it, to:

- Identify and assess laws, Executive Orders, policies, and procedures that apply to protected information that it will make available for ISE dissemination or access.
- Develop policy, as needed, to fill gaps in agency privacy policies and procedures for sharing information in the ISE.
- Document the agency's ISE privacy-related policies and procedures in a written ISE privacy protection policy.
- Identify data holdings that contain protected information that will be shared through the ISE.
- Assess whether the agency's ISE privacy protection policy has been applied to protected information to be shared through the ISE and, if not, apply the policy to the information.
- Establish notice mechanisms that allow ISE participants to identify the nature of the protected information so it can be handled in accordance with applicable legal requirements.
- Implement data quality procedures (accuracy, correction methods, retention).
- Use appropriate security measures to safeguard protected information.

- Hold personnel accountable, provide training, and enable reviews and audits to verify compliance.
- Establish appropriate redress procedures to address complaints from persons regarding information under department or agency control.
- Implement guidelines via training, business process changes, and system design.
- Facilitate public awareness of agency Privacy Guidelines implementation.

The head of each federal agency participating in the ISE has appointed an ISE privacy official responsible to oversee development and implementation of a compliant privacy policy and accountable for compliance with internal policy in the conduct of terrorism information sharing.

How do the ISE Privacy Guidelines relate to the Fair Information Principles, the Privacy Act, and other privacy rules?

The ISE Privacy Guidelines incorporate, to the extent relevant and applicable, privacy principles such as the Fair Information Principles and other privacy best practices. It is important to note that there are many sets of privacy and related rules that apply to different agencies, activities, and data throughout the federal government; a nonexhaustive 2006 compilation of existing rule sets identified 109 sets of rules. These rules provide specific, substantive privacy protections, and agencies must continue to comply with them. Given the diversity and importance of these rules, the drafters of the Guidelines determined that it was neither legally feasible nor desirable to override those rules and protections through the issuance of a "superset" of substantive privacy rules for all agencies, all activities, and all types of data. Instead, the Guidelines require agencies to assess, document, and enforce the rules applicable to the protected information that they seek to access or make available through the ISE and to take other uniform steps to ensure that appropriate safeguards are put in place to guide the development and use of the ISE. This approach enables agencies to adopt tailored protections while preserving statutory privacy and other legal safeguards.

What are the specific privacy rules that an ISE user must follow in accessing the ISE?

The ISE is not a single computer system or database that users access per se. It is a coordinated, centrally led approach to enhancing the sharing of terrorism-related information. An agency's participation in the ISE may, therefore, take different forms. As an agency determines what information it can make available to others and what information it will access, it will be required to assess applicable privacy rules and put in place safeguards appropriate to the type of information and sharing involved.

How were the ISE Privacy Guidelines developed?

The ISE Privacy Guidelines were developed by an interagency working group consisting of federal government privacy officials and subject-matter experts. The drafting process was co-chaired by the Office of the Director of National Intelligence's Civil Liberties Protection Officer and the Chief of the U.S. Department of Justice's Privacy and Civil Liberties Office and included privacy representatives from the members of the Information Sharing Council. For guidance, the group relied on the Fair Information Principles and operating principles contained within the Code of Federal Regulations (CFR), Title 28 (28 CFR), Judicial Administration, Chapter 1—U.S. Department of Justice, Part 23 (28 CFR Part 23). In addition, the group utilized publications by the Markle Foundation, the Center for Democracy and Technology, the Data Privacy and Integrity Advisory Committee of the U.S. Department of Homeland Security (DHS), and the Bureau of Justice Assistance (BJA).

What was the role of the original Privacy and Civil Liberties Oversight Board?

As required by Sections 1016 and 1061 of the IRTPA, the guidelines were developed in consultation with the White House Privacy and Civil Liberties Oversight Board. The Board was consulted as the guidelines were being developed and again during the interagency coordination process.

Federal Agencies

What is our first step for complying with the ISE Privacy Guidelines?

Each agency has already taken the first step by designating an ISE Privacy Official. This milestone was achieved on December 29, 2006.

How will we resolve issues that cut across federal agencies, such as questions about the application of the Privacy Act or about other federal legal requirements that affect more than one agency?

As called for by the ISE Privacy Guidelines, the establishment of an ISE Privacy Guidelines Committee (PGC) was announced by the Program Manager in November 2006. The committee's membership includes the ISE Privacy Officials designated by each of the Federal agencies that are members of the Information Sharing Council. The committee seeks to ensure consistency and standardization in the implementation of the Privacy Guidelines, as well as serve as a forum to share best practices and resolve interagency issues. If an issue cannot be resolved by the PGC, the Program Manager will address the issue through the established ISE governance process. The PGC is not intended to replace legal or policy guidance mechanisms established by law or Executive Order or as part of the ISE and will, as appropriate, work through or in consultation with such other mechanisms.

Who has been designated to chair the ISE Privacy Guidelines Committee?

Pursuant to the PM-ISE's designation, the co-chairs of the ISE Privacy Guidelines Committee are Alexander W. Joel and Kenneth P. Mortensen. Alex Joel is the Civil Liberties Protection Officer for the Office of the Director of National Intelligence. Ken Mortensen is the Acting Chief of the Privacy and Civil Liberties Office of the U.S. Department of Justice. Alex Joel previously co-chaired the interagency working group that drafted the ISE Privacy Guidelines, and Ken Mortensen served as a member of that group, representing the U.S. Department of Homeland Security.

Will we receive additional guidance and support for implementing the ISE Privacy Guidelines?

The ISE Privacy Guidelines Committee (PGC) has played a major role in providing ongoing guidance and support to federal agencies as they implement the Guidelines. In addition, the PM-ISE has funded an implementation support effort via the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. This effort is assisting the Program Manager and the PGC in providing guidance, information, and tools to ISE participants to support their implementation activities. For example, on September 10, 2007, the Program Manager provided the *Privacy and Civil Liberties Implementation Guide for the ISE (Implementation Guide)* to federal agencies. The *Implementation Guide* assists federal agencies in their efforts to ensure that the ISE is established and used in a manner that protects the information privacy and other legal rights of Americans. The *Implementation Guide* describes the processes for ISE participants to follow when integrating privacy and civil liberties safeguards into their information sharing efforts, including an assessment of whether current activities comply with the ISE Privacy Guidelines.

The *Implementation Guide* was developed through a collaborative interagency process by the PGC with the concurrence of the Information Sharing Council and is a further demonstration of the Administration's serious and continued commitment to protect the freedom, information privacy, and other legal rights of Americans in the development and use of the ISE. The ISE PGC is also assisting nonfederal ISE participants to develop and implement similar privacy protections.

Additional information can be found at www.ise.gov.

Can our agency's existing privacy policy comply with the ISE Privacy Guidelines?

Yes, the ISE Privacy Guidelines are designed as a set of core principles to be followed by federal departments and agencies. They require specific, uniform actions and the establishment of a governance structure to develop guidance and foster compliance. Agencies should identify and assess their existing privacy policies and procedures to ensure that they comply with **all** Privacy Guidelines requirements. The agency's ISE privacy official has a leadership role in determining whether the agency's privacy policies and procedures are fully compliant and, if not, establishing new or modified policies and procedures that protect information privacy and other legal rights.

If, as part of the rules assessment process called for in Section 2 of the ISE Privacy Guidelines, my agency finds that a change in its rules would be desirable, what should it do?

The ISE Privacy Guidelines anticipate that as part of its rules assessment, an agency may identify gaps in protections or may find bureaucratic restrictions that do not directly relate to legal requirements. Section 2(c) of the Guidelines sets forth a process for addressing such situations.

How should my agency deal with the legal exemptions that may apply to certain agency activities?

The ISE Privacy Guidelines recognize that certain agencies may enjoy exemptions and exceptions to various privacy protections or other legal requirements. These exemptions reflect public policy determinations made under our system of government. The Guidelines do not override applicable laws or exemptions. However, agencies are expected to review such exemptions as part of the rules assessment process, including evaluating whether the rationale underlying the exemption remains valid in the ISE context or whether any changes to established practice are needed. Agencies may effect such changes in practice pursuant to the process set forth in Section 2(c) of the Guidelines.

What data holdings must be identified and assessed for ISE access?

Agencies are required to identify and assess only those data holdings that contain protected information to be shared through the Information Sharing Environment.

State, Local, and Tribal (SLT) Agencies

Can nonfederal entities participate in the ISE?

Nonfederal entities can participate in ISE information sharing, including state, local, and tribal governments and private sector entities.

Are nonfederal entities required to comply with the ISE Privacy Guidelines?

The ISE Privacy Guidelines apply only to federal agencies and, therefore, do not directly impose obligations on nonfederal entities. However, Section 11 of the ISE Privacy Guidelines requires federal agencies to work with the PM-ISE and with nonfederal entities seeking to access protected information through the ISE to ensure that such nonfederal entities develop and implement "appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in these Guidelines."

How is the federal government helping state, local, and tribal authorities to share information?

State and regional fusion centers are a critical part of how state, local, and tribal authorities share information. Since 2001, the U.S. Department of Homeland Security (DHS) has provided funding via grant programs to support their establishment and the development of a baseline level of capability. The U.S. Department of Justice (DOJ) and DHS have developed extensive training and technical assistance programs to support the establishment and operation of these centers.

In addition, DOJ supports the Global Justice Information Sharing Initiative (Global), which serves as a Federal Advisory Committee (Global Advisory Committee [GAC]), advising the U.S. Attorney General on justice information sharing and integration initiatives. Global facilitates the broad scale, efficient exchange of justice and public safety information and promotes standards-based electronic information exchange to provide the justice community with timely, accurate, complete, and accessible information in a secure and trusted environment.

The GAC represents more than 30 independent organizations, spanning the spectrum of law enforcement, judicial, correctional, and related bodies. Its work is informed by a Criminal Intelligence Coordinating Council (CICC). Composed of members from law enforcement agencies at all levels of government, the CICC was originally established in 2004 to provide advice in connection with the implementation and refinement of the *National Criminal Intelligence Sharing Plan (NCISP)*. Members of the CICC serve as advocates for local law enforcement and support their efforts to develop and share intelligence and information for the purpose of promoting public safety and securing our nation. The work of the GAC and the CICC has had a direct impact on the work of more than 1.2 million justice professionals.

Global initiatives include the development of technology standards, such as the Global Justice XML Data Model (Global JXDM); written products on data sharing issues, such as the *NCISP;* privacy policy development; and many others. Dissemination of information is via the Global Web site, www.it.ojp.gov/index.jsp.

Were state, local, and tribal government officials included in the planning of the ISE?

Yes. There was extensive consultation with and input from state, local, and tribal officials. This interaction included multiple meetings of the Information Sharing Council's State, Local, and Tribal Subcommittee and participation in a number of meetings with key officials and stakeholder groups. State, local, and tribal officials were involved in the drafting of the ISE Implementation Plan Report.

How do state, local, and tribal governments obtain access to protected information in the ISE?

It is anticipated that the main focus of information sharing by federal agencies with state, local, and tribal governments will be via the network of state and regional fusion centers. The PM-ISE will establish a process for ensuring that such fusion centers develop and implement

appropriate policies and procedures for sharing protected federal information and intelligence with state, local, or tribal governments and private sector entities. Federal agencies will continue to disseminate time-sensitive information and other mission-specific information directly to their existing partners as appropriate. However, these direct communications will be coordinated both at the federal level and with the relevant state or regional fusion center. Additional information can be found at www.ise.gov.

What information currently collected and maintained by my SLT agency is protected by the ISE Privacy Guidelines?

As currently configured, the ISE Privacy Guidelines apply only to protected information. For nonintelligence agencies, protected information is defined as information about U.S. citizens and lawful permanent residents (LPRs) that is subject to information privacy or other legal protections under the U.S. Constitution and federal laws of the United States. For the Intelligence Community, protected information includes information about "United States Persons" as defined in Executive Order 12333. It may also include other information that the U.S. government expressly determines by Executive Order, international agreement, or similar instrument should be protected in the ISE. The Guidelines limit the sharing of protected information through the ISE to terrorism information, homeland security information, and law enforcement information.

How does an SLT agency determine what protected information will be shared through the ISE?

The ISE Privacy Guidelines establish a two-part process an agency should undertake to determine what protected information will be shared through the Information Sharing Environment:

1. By applying the definition of protected information to information identified as terrorism-related, the agency will determine whether particular data qualifies for ISE sharing.
2. By applying applicable law and policy, the agency then will determine whether the information can and will be shared through the ISE.

Once these determinations have been made, the specific ISE privacy protections (notice, data quality, security, etc.) must be applied to the data in order for it to be shared through the ISE.

Is our SLT agency-approved privacy policy sufficient for ISE Privacy Guidelines compliance?

The ISE Privacy Guidelines have been developed as a set of core principles for protecting information privacy. Agencies should review their existing privacy policies and procedures to ensure that they embrace these core principles and that they are at least as comprehensive as the Guidelines.

State, local, and tribal government agencies should strive to ensure that their information protection policies and procedures are at least as comprehensive as the ISE Privacy Guidelines. This effort will likely be implemented through processes established by the PM-ISE in conjunction with other federal agencies and state and regional fusion center representatives.

Does compliance with 28 CFR Part 23 enable us to participate in the ISE?

The Fair Information Principles and the operating principles contained within 28 CFR Part 23 were developed for different purposes than the requirements in the ISE Privacy Guidelines. Title 28 CFR Part 23 applies only to the collection, storage, and dissemination of criminal

intelligence information. The Guidelines apply to a broader universe of data. However, if an agency followed a process to become 28 CFR Part 23-compliant that is consistent with the core principles of the Guidelines and has developed procedures that are at least as comprehensive as those required by the Guidelines for all personally identifiable information held by the agency, the agency may be able to participate in the ISE.

Does participation in a statewide fusion center meet the requirements to participate in the ISE?

The PM-ISE, in concert with the U.S. Department of Justice and the U.S. Department of Homeland Security, will establish a process by which entities represented at fusion centers may conform their policies and processes to those required by the ISE Privacy Guidelines for participation in the ISE.

Will SLT agencies that currently share information with federal agencies be able to continue sharing information in light of the ISE Privacy Guidelines?

State, local, and tribal agencies that share a variety of information with federal agencies will be able to continue to share such information provided, of course, that such sharing is permitted by applicable laws and policies. With respect to ISE-protected information subject to sharing, all such agencies must diligently and promptly work toward developing and implementing policies and procedures that provide protections that are at least as comprehensive as those contained in the ISE Privacy Guidelines.

Other Nonfederal Entities

Apart from state, local, and tribal governments, what other nonfederal entities will be participating in the ISE?

IRTPA Section 1016 anticipates sharing by federal departments and agencies with state, local, and tribal governments, private sector entities, and foreign partners and allies.

Are private sector entities involved in the planning of the ISE?

Yes. Efforts to establish the ISE are being coordinated with information sharing activities delineated in the National Infrastructure Protection Plan as well as other efforts already under way by the U.S. Department of Homeland Security, the FBI, the Department of Defense, the Office of the Director of National Intelligence, and other federal entities.

What are the guidelines for sharing with private sector entities?

The ISE Privacy Guidelines establish that federal agencies and the PM-ISE will work with nonfederal entities, including private sector entities, to ensure that they develop and implement information protection policies and procedures that are at least as comprehensive as those contained in the Guidelines. To achieve this result, the PM-ISE is working with the private sector subcommittee of the Information Sharing Council and with other mechanisms established for public/private collaboration, such as those established by the U.S. Department of Homeland Security.

What are the guidelines for sharing with foreign partners?

The ISE Privacy Guidelines do not establish a framework for sharing protected information with foreign partners. Such sharing is addressed in the Guideline 4 Report—*Facilitate Information Sharing Between Executive Departments and Agencies and Foreign Partners*. In consultation with the Information Sharing Council, the PM-ISE's role under IRTPA is to assist in developing policies and issue governmentwide procedures, guidelines, instructions, and functional standards that "(vii) address and facilitate, as appropriate, information sharing between Federal

departments and agencies with foreign partners and allies; and (viii) ensure the protection of privacy and civil liberties." (IRTPA, Section 1016 (f)(2)(B)).

Do the ISE Privacy Guidelines cover personally identifiable information about non-U.S. persons that is made available by foreign partners?

The ISE Privacy Guidelines apply to protected information. The definition of this term explicitly provides that 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 the ISE Privacy Guidelines. Thus, personally identifiable information about non-U.S. persons would be covered by the Guidelines, if such an instrument were to so provide. This provides the U.S. government with the option, acting through appropriate channels, to extend ISE privacy protections to such information.