Information Sharing Environment Privacy Guidelines

Frequently Asked Questions
Version 1.0
Last updated: December 1, 2006

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 Agencies

Other Non-Federal Entities

Definitions

Information Sharing Environment (ISE)—In accordance with the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA), Section 1016, and Executive Order 13388, entitled *Further Strengthening the Sharing of Terrorism Information to Protect Americans*, the Information Sharing Environment (ISE) is defined as the combination of policies, procedures, and technologies linking the resources (people, systems, databases, and information) of all federal executive branch entities to facilitate terrorism information sharing, access, and collaboration among users in order to combat terrorism more effectively. In addition, ISE will provide links to state, local, and tribal government agencies and the private sector to ensure effective sharing of information among all relevant entities. The Information Sharing Environment is designed to meet the dual imperatives of sharing critical information and protecting privacy and civil liberties.

IRTPA—"IRTPA" stands for the *Intelligence Reform and Terrorism Prevention Act of 2004,* Public Law 108-458, 50 USC 401 note. The ISE is covered by Section 1016 of the 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 agency-wide 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 and is composed of each agency's ISE Privacy Official. The Committee provides ongoing guidance on the implementation of these 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, the 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.

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;
- The ability to prevent, interdict, or disrupt terrorist activity;
- The identification or investigation of a suspected terrorist or terrorist organization or any person, group, or entity associated with or assisting a suspected terrorist or terrorist organization; or
- A planned or actual 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;
  - 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.

General Questions About the Information Sharing Environment

What is the Information Sharing Environment (ISE)?

In accordance with the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA), Section 1016, and Executive Order 13388, entitled *Further Strengthening the Sharing of Terrorism Information to Protect Americans*, the Information Sharing Environment (ISE) is defined as the combination of policies, procedures, and technologies linking the resources (people, systems, databases, and information) of all federal executive branch entities to facilitate terrorism information sharing, access, and collaboration among users in order to combat terrorism more effectively. In addition, the ISE will provide links to state, local, and tribal government agencies and the private sector to ensure effective sharing of information among all relevant entities. The ISE is designed to meet the dual imperatives of sharing critical information and protecting privacy and civil liberties.

What is the purpose of establishing the ISE?

At the current time, the sharing of terrorism and other related information takes place within multiple sharing environments within individual communities of interest, including law enforcement; homeland security; state, local, and tribal agencies; defense; intelligence; diplomatic; and the private sector. Over time, each of these communities of interest has

developed its own unique policies, rules, guidelines, standards, architectures, and systems to deliver functionality and capabilities to accomplish specific mission requirements. As a result, the current information sharing environment is not as integrated, interconnected, or robust as the nation requires. The challenge, therefore, is to transform the current environment into one that better facilitates and expedites access to terrorism information and enables the sharing and integration of information across appropriate state, local, tribal, and federal government agencies and private sector entities.

The vision for tomorrow's ISE consists of creating the conditions by which information can be accessed across agency and jurisdictional boundaries and between the federal government and its state, local, and tribal agencies and private sector partners in a timely, efficient, and frictionless manner while protecting the information privacy, civil rights, and other legal rights of Americans.

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

No. The ISE will not result in the construction of a single interconnected computer system touching all levels of government and containing all terrorism information. The ISE will use technology to the maximum extent possible to enhance information sharing.

What information will be shared through the ISE?

The ISE will facilitate the sharing of terrorism information, homeland security information, and certain types of law enforcement information.

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

IRTPA Section 1016 requires the President to designate an individual to serve as the PM-ISE. The PM-ISE's duties include:

- Planning, overseeing the implementation of, and managing the ISE;
- Assisting in the development of policies, procedures, guidelines, rules, and standards, as appropriate to foster ISE development and proper operation; and
- Supporting, monitoring, and assessing the implementation of the ISE by federal departments and agencies, and regularly reporting the findings to the U.S. Congress and the President of the United States (President).

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 and 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 brings to the position an extensive background in national security matters, political-military affairs, counterterrorism, and counternarcotics. Ambassador McNamara is a career diplomat who has served eight Presidents over the past four decades and has most recently served as the Senior Advisor for Counter Terrorism and Homeland Security at the U.S. Department of State. Ambassador McNamara possesses Bachelor of Arts, Master of Arts, and honorary doctoral degrees in history and political science.

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

In June 2005, the President directed that the Office of the PM-ISE be part of the Office of the Director of National Intelligence (ODNI). Although reporting to ODNI, the PM-ISE's mandate covers access to terrorism information across state, local, tribal, and federal government entities and the private sector.

What is the ISE Implementation Plan (ISE IP)?

The *Information Sharing Environment (ISE) Implementation Plan* (ISE IP) 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 entitled *Guidelines and Requirements in Support of the Information Sharing Environment*. The ISE IP designates the actions the federal government intends—in coordination with its state, local, and tribal agencies; the private sector; and foreign partners—to carry out over the next three years. Chapter 9 addresses privacy and civil liberties. A copy of the plan can be found at www.ise.gov.

What is the Governance Structure for the ISE?

There are three primary components to the ISE Governance Structure:

1. Program Manager (PM),
2. Information Sharing Council (ISC), and
3. Information Sharing Policy Coordination Committee (ISPCC).

In addition, the President has established the Privacy and Civil Liberties Oversight Board (PCLOB) to ensure a system of checks and balances in order to protect individual privacy and civil liberties.

The Information Sharing Council is an interagency forum, established by IRTPA Section 1016 and Executive Order 13388 to serve as an advisory body to the President and PM in the development of policies, procedures, and guidelines necessary for ISE implementation. Chaired by the PM, this council acts as a mechanism to ensure coordination among federal departments and agencies and is a means for the Program Manager to assess progress among ISE communities. The ISC has established two subcommittees to address state, local, and tribal agency and private sector issues. These subcommittees are cochaired 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) systems. The Program Manager is also a member of ISPCC.

The 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 requires consultation with 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 work closely with the PCLOB to ensure that privacy and civil liberties are protected throughout ISE development and management. More information about the Board can be found at www.privacyboard.gov.

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?
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) are to be implemented by federal departments and agencies to ensure that the information privacy rights 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. The ISE Privacy Guidelines establish a framework for sharing 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 unique 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 to federal departments and agencies in their development and use of the ISE.

What information is covered by the ISE Privacy Guidelines?
The ISE Privacy Guidelines apply to protected information.

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 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 privacy-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 accountability and audit mechanisms, implement data quality and, where appropriate, redress procedures and identify an ISE Privacy Official to ensure compliance with the 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 relating to civil liberties and the legal rights of Americans in the development and use of the ISE.

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

Due to differing laws, policies, and missions of federal departments and agencies, the Privacy Guidelines use a process approach to determine compliance. This approach requires each department and agency, as required 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;
- Identify data holdings that contain protected information that will be shared through the ISE;
- Ensure that protected information has been reviewed pursuant to the Privacy Guidelines;
- Establish 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 redress procedures to address complaints from persons regarding information under department or agency control;
- Implement guidelines via training, business process changes, and system design; and
- Facilitate public awareness of agency Privacy Guidelines implementation.
- Document the agency's ISE privacy processes and procedures in a privacy policy.

Each agency head must appoint an ISE Privacy Official who will be responsible for overseeing the agency's implementation of and who will be accountable for its compliance with the Privacy Guidelines.

How do the ISE Privacy Guidelines relate to the "Fair Information Practices," 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 Practices 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 review of existing compilations of such rule sets found over 100. These rules provide real, substantive, and tailored privacy protections and agencies must continue to comply with them. Given the diversity and importance of these rules, the drafters of the ISE Privacy Guidelines determined that it was not feasible, legally permissible, or desirable to seek 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 ISE Privacy Guidelines require agencies to assess, document, and enforce the rules applicable to the protected information that they seek to access or make available via the ISE and to take other uniform steps to ensure that appropriate safeguards are put in place in their 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. It is a coordinated, centrally led approach to enhancing the sharing of terrorism 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 appropriate safeguards, tailored for 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 cochaired by the ODNI's Civil Liberties Protection Officer and the Chief of DOJ'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 Practices 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 Privacy and Civil Liberties Oversight Board?
As required by Sections 1016 and 1061 of the IRTPA, the Guidelines were developed in consultation with the Privacy and Civil Liberties Oversight Board. The Board was consulted as the Guidelines were being developed and again during the interagency coordination process. The Board will be consulted on an ongoing basis as part of the ISE Privacy Guidelines governance process. See Section 12(c) of the ISE Privacy Guidelines.

Federal Agencies

What is our first step for complying with the ISE Privacy Guidelines?
Each agency must designate an ISE Privacy Official by December 29, 2006.

How will we resolve issues that cut across federal agencies, such as application of the Privacy Act and other federal legal requirements that affect more than one agency?
As called for by the ISE Privacy Guidelines, the ISE Privacy Guidelines Committee will provide 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. The ISE Privacy Guidelines Committee 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. The ISE Privacy Guidelines Committee consists of the ISE Privacy Officials of each member agency of the Information Sharing Council. If an issue cannot be resolved by the ISE Privacy Guidelines Committee the PM will address the issue through the established ISE governance process.

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

Pursuant to the PM-ISE's designation, the cochairs of the ISE Privacy Guidelines Committee are Alexander Joel and Jane Horvath. Alexander Joel is the Civil Liberties Protection Officer for the Office of the Director of National Intelligence. Jane Horvath is the Chief of the Privacy and Civil Liberties Office of the U.S. Department of Justice. Mr. Joel and Ms. Horvath previously cochaired the interagency working group that drafted the ISE Privacy Guidelines.

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

It is anticipated that the ISE Privacy Guidelines Committee will play a major role in providing ongoing guidance and support to federal agencies as they implement these 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 will provide guidance, information, and tools to ISE participants to support their implementation activities, such as more detailed FAQs, model privacy policies, sample training modules, and the like.

Does our federal agency-approved privacy policy comply with the ISE Privacy Guidelines?

The ISE Privacy Guidelines are designed as a set of core principles to be followed by federal departments and agencies and require specific, uniform actions and the establishment of a governance structure to foster compliance and develop guidance, as appropriate. Agencies should review their privacy policy and procedures to ensure that they comply with **all** Privacy Guidelines requirements. An agency's ISE Privacy Official, who is responsible for agency-wide oversight, will be able to determine whether an agency's privacy policy and procedures are fully compliant and, if not, what steps are required to achieve compliance.

If, as part of the rules assessment process called for in Section 2, my agency finds that a change in 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 ISE Privacy 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 exemptions and exceptions to legal requirements may apply to an agency's participation in the ISE. These exemptions reflect public policy determinations made under our system of government. The ISE Privacy 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 any changes are needed, pursuant to the process set forth in Section 2(c) of the ISE Privacy Guidelines.

For multiple databases, what data holdings must be identified/assessed for ISE access?

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

Apart from privacy, what other legal rights might result in information being deemed "protected information" in the ISE?

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.

State, Local, and Tribal Agencies

Can non-federal entities participate in the ISE?

Non-federal entities (state, local, and tribal governments, private sector entities, and foreign governments) can participate in ISE information sharing. However, federal agencies must work with the PM-ISE and such non-federal entities to ensure they develop and implement appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in these Guidelines.

Are non-federal 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 non-federal entities. However, federal agencies are required to work with the PM-ISE and with non-federal entities seeking to access protected information through the ISE to ensure that such non-federal entities develop and implement appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in these Guidelines.

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 with state, local, and tribal governments will be via the state or regional fusion centers. The PM-ISE will establish a process for ensuring that such fusion centers develop and implement appropriate policies and procedures for protected information when working with state, local, or tribal agencies.

What information currently collected and maintained by my agency fits within the definition of the ISE?

As currently configured, the ISE Privacy Guidelines apply only to protected information. Protected information is defined as information about United States citizens and lawful permanent residents (Americans) that is subject to information privacy or other legal protections under the U.S. Constitution and federal laws of the United States. The ISE Privacy Guidelines limit ISE use of protected information to terrorism information, homeland security information, and certain types of law enforcement information.

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

Non-federal agencies must work toward becoming acknowledged as having policies and procedures at least as comprehensive as the ISE Privacy Guidelines in a timely manner, through the process to be established by the PM-ISE which is likely to be accomplished in conjunction with fusion centers.

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

The Fair Information Practices and the operating principles contained within 28 CFR Part 23 were developed for different purposes than the requirements in the ISE Privacy Guidelines. 28 CFR Part 23 applies only to the collection, storage, and dissemination of criminal intelligence information. The ISE Privacy Guidelines are far broader in scope and deal with protected information regarding all U.S. citizens and lawful permanent residents (Americans) and its use within the ISE context. However, if an agency followed a process to become 28 CFR Part 23-compliant that is consistent with the core principles of the ISE Privacy Guidelines and has developed procedures that are at least as comprehensive as those required by the ISE Privacy Guidelines for all personally identifiable information held by the agency, the agency may be able to participate in the ISE.

In addition, non-federal agencies must work toward becoming acknowledged as having policies and procedures at least as comprehensive as the ISE Privacy Guidelines in a timely manner, through the process to be established by the PM-ISE which is likely to be accomplished in conjunction with fusion centers.

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

The PM-ISE will establish a process for meeting the ISE Privacy Guidelines' privacy requirements that will likely focus on fusion centers.

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

Non-federal agencies that share a variety of information with federal agencies will be able to continue to share such information, provided that such sharing is permitted by applicable laws and policies. All such agencies must, however, 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 Non-Federal Entities

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

As provided in IRTPA Section 1016, the ISE includes sharing by federal departments and agencies not only with state, local, and tribal governments but also with the private sector and foreign partners and allies.

What are the guidelines for sharing with the private sector?

The ISE Privacy Guidelines provide that federal agencies must work with the PM-ISE and non-federal entities, such as private sector entities, to ensure they develop and implement appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in these Guidelines. The PM-ISE will establish a process for meeting this requirement. It is anticipated that this process will include working with the private sector subcommittee of the ISC 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 and allies?

The ISE Privacy Guidelines provide that federal agencies must work with the PM-ISE and foreign partners and allies to ensure they develop and implement appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in these Guidelines. The PM-ISE will establish a process for meeting this requirement.

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

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 these guidelines. Thus, personally identifiable information about non-U.S. persons would be covered by the ISE Privacy Guidelines if such an instrument were to so provide. This provides the U.S. government the option, acting through appropriate channels, of extending ISE privacy protection to such information.