Guideline 5 - Guidelines to Implement Information Privacy Rights and Other Legal Protections in the Development and Use of the Information Sharing Environment

Introduction

In the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Congress directed the establishment of an Information Sharing Environment (ISE) to improve and facilitate the sharing of terrorism information. On December 16, 2005, and in furtherance of his efforts to implement the enactment, the President issued a Memorandum for the Heads of Executive Departments and Agencies, which establishes guidelines and directs particular actions to effect the creation and operation of the ISE.

Guideline Five of the President's Memorandum requires, in relevant part, that the Attorney General and the Director of National Intelligence: "(A) 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 "(B) 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 in the acquisition, access, use, and storage of personally identifiable information."

Information is a vital tool in the Global War on Terror. It helps protect us from terrorist attack only if it is available to the people who need it to perform their missions. We must take care to share terrorism information in a way that preserves the freedoms on which our nation was founded. In the words of the 9/11 Commission: there is a "need for balance as our government responds to the real and ongoing threat of terrorist attacks… [W]hile protecting our homeland, Americans should be mindful of threats to vital personal and civil liberties. This balancing is no easy task, but we must constantly strive to keep it right."[1] Meeting the dual imperatives of protecting privacy and sharing information is at the core of the approach taken to establishing the ISE. The Privacy Guidelines that follow are designed to ensure that information privacy and other legal rights of Americans are protected in the development and use of the ISE.

The Process Used to Complete This Task

The Complex Legal and Mission Environment. Substantive research on existing privacy laws, regulations, executive orders, and departmental policies was completed prior to

[1] 9/11 Commission Report, 394.

preparing the Guidelines. That research identified 108 sets of rules potentially relating to privacy and information sharing.[2] Note that no single agency would have to comply with all these rules – some are agency-specific, while others apply only to certain types of data and activities. The Privacy Guidelines acknowledge the complexity of this legal environment – a complexity that is in part the result of different agency missions – and provide sufficient flexibility to allow each agency and department the ability to tailor implementation to its legal and mission environment. Should an agency believe that a rule is a bureaucratic impediment that serves no privacy purpose, the Privacy Guidelines establish an interagency process for conducting an appropriate review.

The Privacy Recommendation Drafting Process. The ISE Privacy Guidelines were drafted by an interagency working group consisting of Federal government privacy officials and subject matter experts. Most of the drafting was done in a small "core working group" consisting of representatives from the Department of Justice (DOJ), the Director of National Intelligence (DNI), the office of the Program Manager, Information Sharing Environment (PM-ISE), the Office of Management and Budget (OMB), and the Privacy Office of Department of Homeland Security (DHS). Drafts were reviewed with a larger "coordinating committee" consisting of privacy representatives from agencies representing the Information Sharing Council (ISC). Drafts were further coordinated with ISC members and the Information Sharing Policy Coordination Committee (PCC). The drafting process was co-chaired by the DNI's Civil Liberties Protection Officer and the Chief of DOJ's Privacy and Civil Liberties Office. For guidance, the drafters took appropriate account of the fair information practices principles of the Privacy Act, the operating principles contained in the Code of Federal Regulations (28 CFR Section 23.20) for criminal justice systems, and publications by organizations such as the Markle Foundation, the Center for Democracy and Technology, DHS's Data Privacy and Integrity Advisory Committee, and the Bureau of Justice Assistance.

The Product

A Privacy Protection Framework. The recommended Privacy Guidelines would establish a framework for sharing terrorism information in the ISE in a manner that protects privacy and civil liberties. The framework would 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 would establish an ISE privacy governance structure for deconfliction, compliance, and continuous development of privacy guidance.

[2] The group suspended its research into department-specific policies, reasoning that each department and agency would be knowledgeable of its own policies and that identifying such policies in an interagency compendium did not serve a useful purpose. Had such research continued, the total rule sets would number well over 108.

Substantive Protections. The Guidelines provide a consistent framework for identifying information that is subject to privacy protection, assessing applicable privacy rules, implementing appropriate protections, and ensuring compliance. A panoply of laws, directives, and policies provide substantive privacy protections for personally identifiable information. The content of those protections will depend on the rules that apply to particular agencies and the information that they are proposing to share. For example, under Executive Order (EO) 12333, intelligence agencies can only collect, retain, and disseminate information about a "U.S. person" if permitted by applicable law and if the information fits within one of the enumerated categories under EO 12333 (e.g., it constitutes foreign intelligence), and it is permitted under that agency's implementing guidelines approved by the Attorney General. Under the Privacy Act, agencies must publish notices of their systems of records, and sharing of individually identifiable information regarding Americans and lawful permanent residents is subject to certain restrictions. Compliance with these and other laws and policies is, therefore, fundamentally important. However, as described below, the Guidelines do more than direct agencies to comply with the law.

Core Privacy Principles. 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:

- Identify and review the protected information [3] to be shared via the ISE (what is being shared and why);
- Enable ISE participants to determine the nature of the protected information to be shared and its legal restrictions (e.g., "this record contains individually identifiable information about a U.S. citizen");
- Share protected information only to the extent it is terrorism information (purpose specification);
- Assess, document, and comply with all applicable laws and policies;
- Establish data accuracy, quality, and retention procedures;
- Deploy adequate security measures to safeguard protected information;

[3] The ISE Privacy Guidelines apply to information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and laws of the United States. For the intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. 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.

- Implement adequate accountability, enforcement, and audit mechanisms to verify compliance;
- Establish a redress process consistent with legal authorities and mission requirements;
- Implement requirements via appropriate changes to business processes and systems, training, and technology;
- Make the public aware of the agency's policies as appropriate;
- Ensure that non-Federal entities, including State, local, tribal, and foreign governments, can access the agencies' protected information only if they provide comparable protections; and
- Designate a senior official accountable for implementation (ISE Privacy Official).

Privacy Governance. Successful implementation of the Guidelines requires a governance structure, both to monitor compliance and to iterate guideline development as lessons are learned. The Guidelines recommend an ISE Privacy Guidelines Committee, consisting of the Privacy Officials of the departments and agencies comprising the Information Sharing Council (ISC), and chaired by the Program Manager of the ISE or his designee. Working closely with the Privacy and Civil Liberties Oversight Board (Privacy Board), the committee will seek to ensure consistency and standardization (where feasible) in the Guidelines implementation, as well as serve as a forum to share best practices and resolve inter-agency issues. As the ISE develops and specific sharing mechanisms institutionalized, the ISE Privacy Guidelines Committee and the Privacy Board will continually refine privacy guidance.

Ongoing Implementation Support. The Program Manager's office, working closely with the Department of Justice, is funding ongoing implementation support for the Guidelines. An experienced team has been identified, organized, and funded to provide implementation support such as creating and distributing guides, methodologies, and other tools, and providing mechanisms for obtaining feedback, responding to common questions, and sharing best practices and lessons learned.

Guidelines to Implement Information Privacy Rights and Other Legal Protections in the Development and Use of the Information Sharing Environment

1. Background and Applicability.

a. Background. Section 1016(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 (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 …." These Guidelines implement the requirements under the IRTPA and EO 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.

b. Applicability. These Guidelines apply to information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States ("protected information"). For the intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. 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.

2. Compliance with Laws.

a. General. In the development and use of the ISE, all agencies shall, without exception, comply with the Constitution and all applicable laws and Executive Orders relating to protected information.

b. Rules Assessment. Each agency shall implement an ongoing process for identifying and assessing the laws, Executive Orders, policies, and procedures that apply to the protected information that it will make available or access through the ISE. Each agency shall identify, document, and comply with any

legal restrictions applicable to such information. Each agency shall adopt internal policies and procedures requiring it to:

(i) only seek or retain protected information that is legally permissible for the agency to seek or retain under the laws, regulations, policies, and executive orders applicable to the agency; and

(ii) ensure that the protected information that the agency makes available through the ISE has been lawfully obtained by the agency and may be lawfully made available through the ISE.

c. Changes. If, as part of its rules assessment process, an agency:

(i) identifies an issue that poses a significant risk to information privacy rights or other legal protections, it shall as appropriate develop policies and procedures to provide protections that address that issue;

(ii) identifies a restriction on sharing protected information imposed by internal agency policy, that significantly impedes the sharing of terrorism information, homeland security information, or law enforcement information (as defined in Section 13 below) in a manner that does not appear to be required by applicable laws or to protect information privacy rights or provide other legal protections, it shall review the advisability of maintaining such restriction;

(iii) identifies 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, it shall review such restriction with the ISE Privacy Guidelines Committee (described in Section 12 below), and if an appropriate internal resolution cannot be developed, bring such restriction to the attention of the Attorney General and the Director of National Intelligence (DNI). The Attorney General and the DNI shall review any such restriction and jointly submit any recommendations for changes to such restriction to the Assistant to the President for Homeland Security and Counterterrorism, the Assistant to the President for National Security Affairs, and the Director of the Office of Management and Budget for further review.

3. Purpose Specification.

Protected information should be shared through the ISE only if it is terrorism information, homeland security information, or law enforcement information (as

defined in Section 13 below). Each agency shall adopt internal policies and procedures requiring it to ensure that the agency's access to and use of protected information available through the ISE is consistent with the authorized purpose of the ISE.

4. Identification of Protected Information to be Shared through the ISE.

a. Identification and Prior Review. In order to facilitate compliance with these Guidelines, particularly Section 2 (Compliance with Laws) and Section 3 (Purpose Specification), each agency shall identify its data holdings that contain protected information to be shared through the ISE, and shall put in place such mechanisms as may be reasonably feasible to ensure that protected information has been reviewed pursuant to these Guidelines before it is made available to the ISE.

b. Notice Mechanisms. Consistent with guidance and standards to be issued for the ISE, each agency shall put in place a mechanism for enabling ISE participants to determine the nature of the protected information that the agency is making available to the ISE, so that such participants can handle the information in accordance with applicable legal requirements. Specifically, such a mechanism will, to the extent reasonably feasible and consistent with the agency's legal authorities and mission requirements, allow for ISE participants to determine whether:

(i) the information pertains to a United States citizen or lawful permanent resident;

(ii) the information is subject to specific information privacy or other similar restrictions on access, use or disclosure, and if so, the nature of such restrictions; and

(iii) there are limitations on the reliability or accuracy of the information.

5. Data Quality.

a. Accuracy. Each agency shall adopt and implement procedures, as appropriate, to facilitate the prevention, identification, and correction of any errors in protected information with the objective of ensuring that such information is accurate and has not erroneously been shared through the ISE.

b. Notice of Errors. Each agency, consistent with its legal authorities and mission requirements, shall ensure that when it determines that protected information originating from another agency may be erroneous, includes incorrectly merged

information, or lacks adequate context such that the rights of the individual may be affected, the potential error or deficiency will be communicated in writing to the other agency's ISE privacy official (the ISE privacy officials are described in section 12 below).

c. Procedures. Each agency, consistent with its legal authorities and mission requirements, shall adopt and implement policies and procedures with respect to the ISE requiring the agency to:

(i) take appropriate steps, when merging protected information about an individual from two or more sources, to ensure that the information is about the same individual;

(ii) 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

(iii) retain protected information only so long as it is relevant and timely for appropriate use by the agency, and update, delete, or refrain from using protected information that is outdated or otherwise irrelevant for such use.

6. Data Security.

Each agency shall use appropriate physical, technical, and administrative measures to safeguard protected information shared through the ISE from unauthorized access, disclosure, modification, use, or destruction.

7. Accountability, Enforcement and Audit.

a. Procedures. Each agency shall modify existing policies and procedures or adopt new ones as appropriate, requiring the agency to:

(i) have and enforce policies for reporting, investigating, and responding to violations of agency policies relating to protected information, including taking appropriate action when violations are found;

(ii) provide training to personnel authorized to share protected information through the ISE regarding the agency's requirements and policies for collection, use, and disclosure of protected information, and, as appropriate, for reporting violations of agency privacy-protection policies;

(iii) cooperate with audits and reviews by officials with responsibility for providing oversight with respect to the ISE; and

(iv) designate each agency's ISE privacy official to receive reports (or copies thereof if the agency already has a designated recipient of such reports) regarding alleged errors in protected information that originate from that agency.

b. Audit. Each agency shall implement adequate review and audit mechanisms to enable the agency's ISE privacy official and other authorized officials to verify that the agency and its personnel are complying with these Guidelines in the development and use of the ISE.

8. Redress.

To the extent consistent with its legal authorities and mission requirements, each agency shall, with respect to its participation in the development and use of the ISE, put in place internal procedures to address complaints from persons regarding protected information about them that is under the agency's control.

9. Execution, Training, and Technology.

a. Execution. The ISE privacy official shall be responsible for ensuring that protections are implemented as appropriate through efforts such as training, business process changes, and system designs.

b. Training. Each agency shall develop an ongoing training program in the implementation of these Guidelines, and shall provide such training to agency personnel participating in the development and use of the ISE.

c. Technology. Where reasonably feasible, and consistent with standards and procedures established for the ISE, each agency shall consider and implement, as appropriate, privacy enhancing technologies including, but not limited to, permissioning systems, hashing, data anonymization, immutable audit logs, and authentication.

10. Awareness.

Each agency shall take steps to facilitate appropriate public awareness of its policies and procedures for implementing these Guidelines.

11. Non-Federal Entities.

Consistent with any standards and procedures that may be issued to govern participation in the ISE by State, tribal, and local governments and private sector entities, the agencies and the PM-ISE will work 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.

12. Governance.

a. ISE Privacy Officials. Each 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 OMB Memorandum M-05-08 dated February 11, 2005), shall directly oversee the agency's implementation of and compliance with these Guidelines (the "ISE privacy official"). If a different official would be better situated to perform this role, he or she may be so designated by the head of the agency. The ISE privacy official role may be delegated to separate components within an agency, such that there could be multiple ISE privacy officials within one executive department. The ISE privacy official shall be responsible for ensuring that (i) the agency's policies, procedures, and systems are appropriately designed and executed in compliance with these Guidelines, and (ii) changes are made as necessary. The ISE privacy official should be familiar with the agency's activities as they relate to the ISE, possess all necessary security clearances, and be granted the authority and resources, as appropriate, to identify and address privacy and other legal issues arising out of the agency's participation in the ISE. Such authority should be exercised in coordination with the agency's senior ISE official.

b. ISE Privacy Guidelines Committee. All agencies will abide by these Guidelines in their participation in the ISE. The PM shall establish a standing "ISE Privacy Guidelines Committee" to provide 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 inter-agency basis. The ISE Privacy Guidelines Committee is not intended to replace legal or policy guidance mechanisms established by law, 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 shall be chaired by the PM or a senior official designated by the PM, and will consist of the ISE privacy officials of each member 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. The ISE Privacy Guidelines Committee should request legal or policy guidance on questions relating to the implementation of these Guidelines from those agencies having responsibility or authorities for issuing guidance on such questions; any such requested guidance shall be provided promptly by the appropriate agencies. As the ISE governance process evolves, if a different entity is established or identified that could more effectively perform the functions of the ISE Privacy Guidelines Committee, the ISE Privacy Guidelines Committee structure shall be modified by the PM through such consultation and coordination as may be required by the ISE governance process, to ensure the functions and responsibilities of the ISE Privacy Guidelines Committee remain priorities fully integrated into the overall ISE governance process.

c. *Privacy and Civil Liberties Oversight Board.* The Privacy and Civil Liberties Oversight Board (PCLOB) should be consulted for ongoing advice regarding the protection of privacy and civil liberties in agencies' development and use of the ISE. To facilitate the performance of the PCLOB's duties, the ISE Privacy Guidelines Committee will serve as a mechanism for the PCLOB to obtain information from agencies and to provide advice and guidance consistent with the PCLOB's statutory responsibilities. Accordingly, the ISE Privacy Guidelines Committee should work in consultation with the PCLOB, whose members may attend Committee meetings, provide advice, and review and comment on guidance as appropriate.

d. *ISE Privacy Protection Policy*. Each agency shall develop and implement a written ISE privacy protection policy that sets forth the mechanisms, policies, and procedures its personnel will follow in implementing these Guidelines. Agencies should consult with the ISE Privacy Guidelines Committee as appropriate in the development and implementation of such policy.

13. General Provisions.

a. Definitions.

(i) 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.

(ii) The term "protected information" has the meaning set forth for such term in paragraph 1(b) of these Guidelines.

(iii) The terms "terrorism information," "homeland security information," and "law enforcement information" are defined as follows:

"Terrorism information," consistent with section 1016(a)(4) of IRTPA means all 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, or 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.

"Homeland security information," as derived from section 482(f)(1) of the Homeland Security Act of 2002, means any information possessed by a Federal, State, local, or tribal agency that relates to (A) a threat of terrorist activity, (B) the ability to prevent, interdict, or disrupt terrorist activity, (C) 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 (D) a planned or actual response to a terrorist act.

"Law enforcement information" for the purposes of the ISE means any information obtained by or of interest to a law enforcement agency or official that is (A) related to terrorism or the security of our homeland and (B) 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 counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, 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.

b. The treatment of information as "protected information" under these Guidelines 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. Heads of executive departments and agencies shall, to the extent permitted by law and subject to the availability of appropriations, provide the cooperation, assistance, and information necessary for the implementation of these Guidelines.

d. These Guidelines:

(i) shall be implemented in a manner consistent with applicable laws and executive orders, including Federal laws protecting the information privacy rights and other legal rights of Americans, and subject to the availability of appropriations;

(ii) shall be implemented in a manner consistent with the statutory authority of the principal officers of executive departments and agencies as heads of their respective departments or agencies;

(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) are intended only to improve the internal management of the Federal Government and are not intended to, and do not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its departments, agencies, or entities, its officers, employees, or agencies, or any other person.

Conclusion

Protecting privacy and civil liberties is a core tenet of the ISE. The ISE Privacy Guidelines provide the framework for enabling information sharing while protecting privacy and other legal rights. To achieve this, the Guidelines strike a balance between consistency and customization, substance and procedure, oversight, and flexibility. The Guidelines build upon existing resources within executive agencies and departments for implementation. The Guidelines are critical to creating the trusted information sharing environment that is the ISE.

Recommendation

It is recommended that the above Guidelines be accepted and issued.