Department of Justice Privacy, Civil Rights, and Civil Liberties Protection Policy for the Information Sharing Environment

January 25, 2010

I. Background

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) directed the President to establish "an approach that facilitates the sharing of terrorism information," which includes information about weapons of mass destruction, homeland security information, and law enforcement information (referred to collectively as "terrorism-related information"), among and between federal, state, local, and tribal agencies and entities, the private sector, and our foreign partners in order to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism on the United States.[1] This approach to information sharing is called the Information Sharing Environment (ISE). IRTPA also directed the President to develop and adopt policies and procedures governing the use of information in the ISE, including guidelines to "protect privacy and civil liberties in the development and use of the ISE."[2]

To that end, the President's Program Manager for the ISE issued the ISE Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the ISE (Privacy Guidelines). The Privacy Guidelines require relevant entities to develop and implement a written privacy

[1] Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 108-458, 18 Stat. 3665, § 1016(a)(2) (Dec. 17, 2004).

[2] IRTPA at § 1016(b)(1). *See* An Introduction to the ISE Privacy Guidelines (Dec. 4, 2006), *available at* http://www.ise.gov/docs/privacy/PrivacyGuidelines20061204.pdf. *See also* ISE Goals, *available at* http://www.ise.gov/pages/vision.html.

protection policy that is at least as comprehensive as the Privacy Guidelines.[3] This document constitutes the Department of Justice's ISE Privacy and Civil Liberties Protection Policy (DOJ ISE Privacy Policy or Policy).

II. Authorities

Privacy Act of 1974 (5 U.S.C. § 522a, as amended); Intelligence Reform and Terrorism Prevention Act of 2004, as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007 (50 U.S.C. § 402 *et seq.*); Executive Order 12333, as amended; Executive Order 13388, as amended; Presidential Memorandum dated December 16, 2005 (*Guidelines and Requirements in Support of the Information Sharing Environment*); and other applicable guidance, policies, orders, directives, and provisions of law. (*See* Appendix B.)

III. Applicability

The DOJ ISE Privacy Policy applies to "protected information," which the ISE defines as "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."[4] Protected information may also include information designated for privacy or other protections by Executive Order, international agreement, or other similar instrument. All DOJ protected terrorism-related information used in the ISE will be treated in accordance with the Policy, which will apply to all DOJ employees, detailees, contractors, and others who have access to DOJ protected terrorism-related

[3] *See* Guidelines to Ensure That the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the ISE (Dec. 4, 2006), *available at* http://www.ise.gov/docs/privacy/PrivacyGuidelines20061204.pdf. (hereinafter ISE Guidelines to Ensure Information Privacy)

[4] *Id.*

information or systems that may be used to share protected terrorism-related information. The Policy must also be incorporated into agreements with foreign partners, private partners, and other governmental entities to the extent that the agreements involve the sharing of protected terrorism-related information.

IV. Compliance with Laws

DOJ complies with the United States Constitution and all applicable laws and Executive Orders related to protected information. The DOJ ISE Privacy Policy will assist those who use DOJ information systems and who collect, maintain, access, use, and share protected information, in complying with all applicable laws, Executive Orders, guidelines, policies and procedures related to privacy and civil liberties.

In accordance with Executive Order 12333 and the Attorney General's Guidelines for Domestic FBI Operations,[5] DOJ is not authorized to collect or maintain information about US persons solely for the purpose of monitoring activities protected by the Constitution, such as the First Amendment protected freedoms of religion, speech, press, and peaceful assembly and protest. Further, DOJ does not collect or retain information based solely on race, ethnicity, national origin, or religious affiliation.[6] The Privacy Act restricts the maintenance of records relating to how protected individuals exercise rights guaranteed by the First Amendment, unless such information is pertinent to and within

[5] *See* United States Department of Justice, Attorney General Guidelines for Domestic FBI Operations (September 29, 2008) (stating the "Guidelines do not authorize investigating or collecting or maintaining information on United States persons solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or the laws of the United States"), *available at* http://www.usdoj.gov/ag/readingroom/guidelines.pdf.

[6] *See, e.g.*, Federal Bureau of Investigation Domestic Intelligence and Operations Guide (DIOG) (December 2008).

the scope of an authorized law enforcement activity or is otherwise authorized by statute.[7]

Compliance Enforcement

A. As a general matter, all DOJ Components that collect, store, use, share, or otherwise handle protected terrorism-related information in the ISE will be required to implement this Policy. Such Components shall designate a senior official (or officials) to serve as the Component's ISE Privacy Official, who will be responsible for the Component's implementation of and compliance with this Policy.

B. DOJ's Chief Privacy and Civil Liberties Officer (CPCLO) serves as DOJ's ISE Privacy Official and, through the Office of Privacy and Civil Liberties (OPCL), which reports to the CPCLO, and through the Components' ISE Privacy Officials, shall oversee DOJ's implementation of and compliance with the DOJ ISE Privacy Policy. Components' ISE Privacy Officials, through consultation with the CPCLO and OPCL, shall be responsible for:

(1) Developing and conducting training to ensure compliance with the DOJ ISE Privacy Policy;

(2) Ensuring that all Memoranda of Understanding entered into for the sharing of terrorism-related information require the contracting parties to adhere to the DOJ ISE Privacy Policy (or to a policy at least as comprehensive); and

(3) Reviewing and assessing complaints and providing redress, as described below, where appropriate.

C. The CPCLO is a co-chair of the Privacy, Civil Rights, and Civil Liberties Information Sharing Committee (Privacy ISC), which is a subcommittee of the

[7] *See* 5 U.S.C. § 552a(e)(7) (2009).

Information Sharing and Access Interagency Policy Committee. The Privacy ISC issued and oversees implementation of the Privacy Guidelines on which this Policy is based, and will coordinate with the President's Privacy and Civil Liberties Oversight Board (PCLOB) on oversight of DOJ's ISE-related activities.

The CPCLO will coordinate with the Department's Law Enforcement Information Sharing Program (LEISP) Coordinating Committee (LCC) (of which the CPCLO is a member) and with the Components' ISE Privacy Officials to review Components' implementation and enforcement of the Policy and, when appropriate, identify and assess the laws, Executive Orders, policies, and procedures that apply to protected information available through the ISE.

The LCC and the Components' ISE Privacy Officials will (1) identify issues that pose significant risks to the privacy of protected information; (2) develop appropriate policies and procedures to address these issues; (3) identify restrictions imposed by internal DOJ policies that significantly impede the sharing of terrorism-related information in a manner that does not appear to be required by applicable laws or to protect the privacy of protected information; (4) evaluate whether changes to such policies are needed to facilitate and ensure the sharing of terrorism-related information; and (5) review restrictions of the type described above imposed by requirements *other* than internal DOJ policy. If the LCC and Components' ISE Privacy Officials, after consultation with the Privacy ISC, are unable to resolve an issue, the CPCLO will bring such restriction to the attention of the Attorney General and the Director of National Intelligence (DNI) for resolution, pursuant to the ISE Privacy Guidelines.

V. Purpose Specification and Identification of Protected Information Shared within the ISE

Protected information may only be shared within the ISE if it is terrorism-related information. All DOJ Components that share terrorism-related information that is also protected information shall ensure that the Component's access to and use of protected information within the ISE is consistent with the authorized purpose of the ISE.

All DOJ system managers will identify systems that contain "protected information" and will implement procedures to ensure protected information is reviewed pursuant to Sections V, VI, and VII of the Policy before such information is made available in the ISE. System managers shall provide sufficient details to recipients of protected information made available through the ISE to enable recipients to determine (1) whether the information is subject to specific privacy or civil liberties requirements, (2) whether there are any limitations on the reliability or accuracy of the information, and (3) whether the information pertains to a US person (including a legal permanent resident) or a non-US person who is protected by treaty or an international agreement.[8]

VI. Data Security

DOJ has physical, technical, and administrative procedures to safeguard protected information from inappropriate, unlawful, and unauthorized access, use, disclosure, or destruction. DOJ's Chief Information Officer (CIO) has implemented an information security program to ensure compliance with the Federal Information Security Management Act of 2002 (FISMA). DOJ Components sharing protected information through the ISE may consult with the CIO to determine the feasibility of additional

[8] Some Components, as a matter of policy, may treat all information as US person information, unless there is reason to believe otherwise.

privacy enhancing technologies, such as data anonymization, authorized use systems or other access controls, and immutable audit logs. Components may adopt additional privacy enhancing technologies to satisfy the requirements of the DOJ ISE Privacy Policy.

VII. Data Quality

Although many of DOJ's information systems are exempt from the data accuracy requirement of the Privacy Act when information is collected, DOJ Components will make reasonable efforts, in the interest of fairness and consistent with DOJ's mission, to ensure the accuracy and completeness of data shared through the ISE. To that end, DOJ Components shall develop and implement policies and procedures to facilitate, to the extent feasible, the prevention, identification, and correction of any errors in protected information shared through the ISE and to ensure that such information has not been shared erroneously through the ISE.[9]

Data Quality Review: Components that make data available for sharing through the ISE will review protected information before it is shared to assess its accuracy and to make reasonable efforts to prevent, identify, and correct errors. In particular, Components, through established processes, will make reasonable efforts to ensure (1) protected information merged from two or more sources relates to the same individual; (2) errors and inconsistencies are investigated and corrected in a timely manner; (3) outdated or irrelevant information is updated or deleted in a timely manner; and (4) data that is pending correction, updating, or deletion is withheld from disclosure or access. If

[9] Note that when DOJ Components disseminate protected information through the ISE to a recipient other than an agency, as defined in 5 U.S.C. § 552(f), they are required to "make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes." 5 U.S.C. § 552a(e)(6).

a Component determines that data quality reviews it currently conducts are sufficient to meet this requirement, it can use those existing procedures. If a Component cannot determine the accuracy of information it makes available in the ISE, the Component will indicate in a data field accompanying the information that the information's reliability and accuracy cannot be verified or is in question and explain why.

Procedures for Errors in Data Received: When the Department 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 Component shall communicate the potential error or deficiency in writing to the other agency's ISE Privacy Official (or other official identified in the applicable Memorandum of Understanding (MOU) or other instrument governing sharing of information).

Procedures for Errors in Data Disseminated: When a Component determines that it is the source of protected information that may be erroneous or may have been shared in violation of policy or statute, and knows or believes the information was accessed through the ISE by another agency, the Component shall (1) maintain a written description of the information, the deficiency and an assessment of the extent of dissemination; (2) notify recipients of the information, to the extent they can be identified, and provide them with the information necessary to clarify the information or properly handle the information; (3) correct, delete, or take other necessary steps to correct the deficiency; and (4) when necessary under Executive Order 12333, report the erroneous dissemination to the Intelligence Oversight Board. (Nothing in this paragraph is intended to duplicate existing statutory requirements.) The Department's information

sharing MOUs reflect agreements and policies to act only on information that has been verified by the originating source. The Department should ensure that its MOUs provide for all of the procedures delineated above.

Procedures for Erroneous Dissemination: If a Component discovers that it has shared protected information erroneously or in violation of this Policy, it shall (1) take action to prevent further sharing of the protected information; (2) recall the disseminated information by contacting all recipients, to the extent they can be identified, to request immediate destruction of all disseminated copies of the information; (3) in the event of a breach (as opposed to an instance of erroneous dissemination), follow procedures outlined in the DOJ *Incident Response Procedures for Data Breaches Involving Personally Identifiable Information* (DOJ Incident Response Procedures) and report the incident to DOJ Computer Emergency Readiness Team, in accordance with the DOJ Incident Response Procedures.

VIII. Redress

Individuals are provided with notice of both the collection of information by the Department and of the possible opportunity to seek access and amendment of protected information through the publication of a system of records notice in the Federal Register and through the Department's website, which posts all of the Department's system of records notices.[10] All DOJ system notices are available through links at the following website: www.justice.gov/opcl/privacyact.html.

Although many of DOJ's information systems are exempt from the access and amendment provisions of the Privacy Act, DOJ Components nonetheless should

[10] *See* http://www.usdoj.gov/opcl/privacyact.html.

implement reasonable measures to respond to individuals' claims that data pertaining to them is inaccurate and, where appropriate, annotate the individuals' records accordingly.

To that end, an individual may request amendment of protected information through a request to the DOJ Component that maintains the system of records containing the individual's information, in accordance with the procedures outlined in DOJ regulations and system notices. Components will make best efforts to determine whether the information about the individual is inaccurate or deficient, where feasible, and may correct inaccurate or deficient information and/or add a statement of disagreement to the complainant's file.

If the individual is unsatisfied with a Component's response to the request, the individual may appeal access requests to the Department's Office of Information Policy[11] and may appeal amendment requests to OPCL.[12] The relevant office will perform a thorough legal analysis to determine whether the initial response to the individual's request was appropriate. Instructions for filing an appeal are provided in DOJ's regulations, 28 C.F.R. §§ 16.9 and 16.45-46, and in the Component's response letter. After a determination has been made, the relevant office will provide the individual with a written response.

If the individual is still unsatisfied with the Department's response, the individual may seek judicial review, pursuant to the Privacy Act and/or the Freedom of Information Act. When redress under the Privacy Act is unavailable because a particular system of

[11] *See* 28 C.F.R. § 16.45 (2008). Although the regulations currently indicate that the Office of Information Privacy handles access requests, the Office of Information Privacy recently changed its name to the Office of Information Policy. This change will be reflected in future Department regulations.

[12] *See* 28 C.F.R. § 16.46 (2008). Although the regulations currently indicate that the Office of Information Privacy handles amendment appeals, this function was recently transferred to OPCL and will be reflected in future Department regulations.

records is exempt from the Privacy Act's amendment provisions, the individual may nonetheless file a statement of disagreement with the relevant Component and request the statement be included in the individual's file.

The DOJ ISE Privacy Policy is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise against DOJ or its officers, employees, agents, or other associated personnel.

VII. Accountability/Enforcement/Audit

Each Component will ensure that it has policies and procedures in place to investigate, respond to, and report violations of this policy. Components' ISE Privacy Officials will notify the CPCLO and OPCL as soon as possible of any significant violations that involve the erroneous use or dissemination of protected information or the use or dissemination of erroneous protected information.

Components' ISE Privacy Officials will design and implement procedures for auditing the sharing of protected information in the ISE. The Components will submit these procedures to the CPCLO for review and approval.

The CPCLO is a co-chair of the ISE Privacy Guidelines Committee, which issued the Privacy Guidelines on which this policy is based and which oversees the implementation of agencies' ISE privacy policies. The CPCLO provides the President's Privacy and Civil Liberties Oversight Board (PCLOB) and Congress with quarterly reports on certain privacy related activities pursuant to Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007. In addition, the CPCLO, through the ISE Privacy Guidelines Committee, will consult with the PCLOB on a regular basis regarding the Department's protection of privacy and civil liberties in the

ISE. Finally, the Department's Office of Inspector General regularly reviews DOJ's activities and programs to ensure compliance with applicable laws and policies.

VIII. Training and Awareness

The CPCLO, through OPCL and ISE Privacy Officials for relevant Components will ensure that all DOJ personnel, detailees, assignees, and contractors who collect, use, and disseminate protected information that is terrorism-related information receive mandatory training program. The CPCLO, through OPCL and the ISE Privacy Officials for relevant Components, will be responsible for ensuring the awareness and implementation of the DOJ ISE Privacy Policy to relevant Components throughout the Department. The CPCLO will ensure the training program is modified as necessary to address technological, statutory, regulatory, or policy changes that impact the collection, use, and dissemination of protected information that is terrorism-related information.

Appendix A – Definitions

Protected Information: "Protected information" is defined in the ISE Privacy Guidelines to mean information about United States citizens and lawful permanent resident aliens (collectively, US persons) that is subject to information privacy or other legal protections under the US Constitution and federal laws. "Protected information" may also include information expressly designated for privacy protection by Executive Order, international agreement, or other similar instrument. 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.

For the Intelligence Community, "protected information" includes information about US persons as defined in Executive Order 12333, which provides that a US 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 US 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.

Terrorism Information: "Terrorism information" is defined in IRTPA Section 1016(a)(4) to mean all information 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: "Homeland security information," as derived from Homeland Security Act of 2002, Pub. L. 107-296, Section 892(f)(1), means any information held 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: "Law enforcement information" for 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 homeland security 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 (as defined in Executive Order 12333 Part 3.5(e)), 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.

Weapons of Mass Destruction (WMD) Information: WMD Information is defined in IRTPA 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 a terrorist organization against the United States.

Terrorism-Related Information: "Terrorism-related information" includes "terrorism information," "homeland security information," and "law enforcement information," as defined above.

Information Sharing Environment (ISE): The ISE is an approach for sharing "protected information" contained in terrorism-related information (including information related to weapons of mass destruction, homeland security information, and law enforcement information related to terrorism) with federal, state, local, and tribal governmental entities, private sector entities, and foreign partners. The ISE is mandated by Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) and is composed of the policies, procedures, protocols, and technologies that govern the handling and management of "protected information" that is subject to exchange with other public and private sector entities and with foreign partners.

DOJ Components: DOJ Components include the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), and any other division, bureau or similar entity that is part of DOJ and shares protected terrorism-related information.

Appendix B – References and Authorities

Legislation

Privacy Act of 1974, 5 U.S.C. §§ 552a *et seq.,* as amended

Freedom of Information Act, 5 U.S.C. §§ 552 *et seq.,* as amended

E-Government Act of 2002, Pub. L. 107-347, 44 U.S.C. Ch. 36

Federal Information Security Management Act of 2002, 44 U.S.C. § 3541 *et seq.*

Intelligence Reform and Terrorism Prevention Act of 2004, as amended, Pub. L. 108-458, Dec. 17, 2004

Implementing Recommendations of the 9/11 Commission Act of 2007, 50 U.S.C. §§ 402 *et seq*.

Executive Orders

Executive Order 12333, *United States Intelligence Activities* (Dec. 4, 1981), as amended

Executive Order 13311, *Homeland Security Information Sharing* (July 29, 2003)

Executive Order 13353, *Establishing the President's Board on Safeguarding Americans' Civil Liberties* (Aug. 27, 2004)

Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans* (Oct. 25, 2005)

Presidential Guideline, *Designation and Sharing of Controlled Unclassified Information (CUI)* (May 9, 2008)

Policies, Guidance, and Other References

Attorney General Guidelines for Domestic FBI Operations (November 2008)

FBI Domestic Investigations and Operations Guide (DIOG) (December 2008)

Intelligence Community Directive Number 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community* (Jan. 21, 2009)

Director of Central Intelligence Directive (CID) 6/3, *Protecting Sensitive Compartmented Information within Information Systems*

OMB Memorandum M-05-08, *Appointments of Senior Agency Officials for Privacy* (Feb. 11, 2005)

OMB Memorandum M-03-02, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Sept. 30, 2003)

OMB Memorandum M-01-05, *Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy* (Dec. 20, 2000)

OMB Memorandum M-99-05, *Instructions on Complying with President's Memorandum of May 14, 1998 – "Privacy and Personal Information in Federal Records"* (Jan. 7, 1999)

DOJ Incident Response Procedures for Data Breaches Involving Personally Identifiable Information, Ver. 1.6 (Aug. 7, 2008)

Privacy and Civil Liberties Policy Development Guide and Implementation Templates, Global Justice Information Sharing Initiative, Department of Justice (February 2008)

Memorandum of Understanding on Terrorist Watchlist Redress Procedures