U.S. Department of Justice

THE DEPARTMENT OF JUSTICE
2011 ANNUAL PRIVACY REPORT

MAY 2012

Message from the Chief Privacy and Civil Liberties Officer

Nancy C. Libin
Chief Privacy and Civil Liberties Officer
Department of Justice

I am pleased to present the Department of Justice's 2011 Annual Report detailing the activities of the Chief Privacy and Civil Liberties Officer (CPCLO) and the Office of Privacy and Civil Liberties (OPCL), in accordance with Section 1174 of Public Law 109-162, the Violence Against Women and Department of Justice Reauthorization Act of 2005. This report covers the reporting periods between 2009 through 2011, which include the transition period for this Administration and my appointment as the Justice Department's CPCLO on June 1, 2009. Because I became CPCLO shortly before the 2009 report was due and in light of the structural changes of the Department's privacy program since my appointment, we have combined the material for these reporting periods to provide a more comprehensive overview of the Department's privacy-related activities during this timeframe with a view toward the future of the Department's privacy program.

The CPCLO serves as the principal advisor to the head of the Department on privacy policy with respect to the Department's collection, use, storage, and disclosure of personal information and when the Department proposes, develops, and implements laws, regulations, policies, procedures, and guidelines related to its counterterrorism efforts. As described in prior annual reports, the CPCLO, with the support of OPCL, fulfills this mission through the regular review and oversight of Departmental programs (including Privacy Act and E-Government Act compliance matters) and participation in policy development at the Department and in interagency and international privacy policy efforts.

As explained fully in this Annual Report, I have been involved in a variety of domestic and international privacy policy matters, including the establishment of nationwide information sharing programs and the negotiation of international data protection agreements. In addition to ensuring the Department's compliance with privacy laws and regulations, OPCL has contributed significantly during this period to the privacy policies governing the Department's adoption and use of social networking technologies, in fulfillment of the President's mandate to make government more transparent, participatory, and collaborative.

We look forward to continuing this important work as the Department fulfills its mission to protect and serve the American public.

Table of Contents

I. BACKGROUND

A. THE CHIEF PRIVACY AND CIVIL LIBERTIES OFFICER

The Department of Justice (Department or DOJ) appointed its first Chief Privacy and Civil Liberties Officer (CPCLO) in 2006 pursuant to the Violence Against Women and Department of Justice Reauthorization Act of 2005. The CPCLO is part of the Office of the Deputy Attorney General (ODAG) and serves as the principal advisor to the head of the Department on privacy policy with respect to the Department's collection, storage, use, and disclosure of personally identifiable information, and advises the head of the Department on privacy issues when the Department proposes, develops, and implements laws, regulations, policies, procedures, or guidelines related to its counterterrorism efforts.[1] Additionally, the CPCLO is responsible for advising the Attorney General on the "implementation of policies and procedures, including appropriate training and auditing, to ensure the Department's compliance with privacy-related laws and policies, including section 552a of title 5, United States Code [the Privacy Act of 1974], and Section 208 of the E-Government Act of 2002 (Public Law 107-347)."[2] The Department appointed Nancy C. Libin as its second CPCLO on June 1, 2009.

During this reporting period, the CPCLO has built upon the activities that the previous CPCLO began by developing privacy policies for the Department's domestic and international information sharing programs and working to establish the Office of Privacy and Civil Liberties as a separate office to manage and oversee all of the Department's privacy compliance and legal work.

B. THE OFFICE OF PRIVACY AND CIVIL LIBERTIES

Since appointing its first statutorily mandated CPCLO, the Department has taken steps to streamline its privacy operations. To that end, the Department established the Office of Privacy and Civil Liberties (OPCL) as a separate office in 2008 to consolidate its privacy compliance and legal work and to provide consistency and leadership to all Department components on information privacy issues.

OPCL is headed by a Director, who reports directly to the CPCLO in ODAG.[3] The Office supports the CPCLO's statutory duties by implementing and coordinating the

[1] *See* Violence Against Women and Department of Justice Reauthorization Act of 2005 § 1174, 28 U.S.C. § 509 (note) (2006); *see also* Implementing Recommendations of the 9/11 Commission Act of 2007 § 803, 42 U.S.C. § 2000ee-1 (2006).
[2] Violence Against Women and Department of Justice Reauthorization Act of 2005 § 1174, 28 U.S.C. § 509 (note) (2006).
[3] OPCL was comprised of eight full-time equivalent employees in fiscal year 2009, eight full-time equivalent employees in fiscal year 2010, and six full-time equivalent employees in fiscal year 2011.

Department's privacy compliance and legal program. OPCL's principal mission is to ensure that the Department complies with federal information privacy laws, regulations, and policies in all its programs and information systems. OPCL accomplishes this by:

- Developing and providing legal guidance to Department components to ensure they comply with federal information privacy laws, regulations, and policies;
- Reviewing and finalizing all Department privacy documentation, including system of records notices and accompanying exemption regulations pursuant to the Privacy Act of 1974, and privacy impact assessments pursuant to Section 208 of the E-Government Act of 2002;
- Reviewing legislative proposals pertaining to privacy issues that impact the Department's handling of information;
- Adjudicating Privacy Act amendment appeals of denials/actions by Department components;
- Publishing the *Overview of the Privacy Act of 1974*, a treatise of Privacy Act case law;
- Establishing and providing annual and specialized privacy compliance, legal, and awareness training to Department personnel;
- Responding to privacy and civil liberties inquiries from the public; and
- Preparing quarterly and annual reports in accordance with Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, the Federal Information Security Management Act of 2002, and Section 1174 of the Violence Against Women and Department of Justice Reauthorization Act of 2005.

Some highlights of OPCL's accomplishments during this reporting period include streamlining the Department's privacy compliance process by establishing the Initial Privacy Assessment (IPA) process. The IPA is a tool for Department components to use to identify information privacy issues as a Department system or program is being developed, as required by the Privacy Act of 1974, the privacy provisions of the E-Government Act of 2002, and other federal privacy requirements. OPCL also published the 2010 edition of the Department of Justice's *Overview of the Privacy Act of 1974*, a widely used treatise of Privacy Act case law. It looks forward to publishing the 2012 edition this year.

During this reporting period, OPCL also actively worked with the CPCLO and other Department leadership to continue to structure the Department's privacy program and to

define OPCL's roles and responsibilities, as well as the privacy roles of the Department components and offices that OPCL supports. As OPCL interacts with all Department components in its compliance and legal work, its staff is able to work collaboratively with Department component privacy officers, information technology (IT) security personnel, and program officials in order to provide and coordinate the appropriate level of privacy expertise and review of DOJ systems and programs. This collaborative environment has allowed OPCL to improve the efficiency and quality of DOJ's privacy compliance work on a department-wide level and to provide the CPCLO with ideas for continued improvements and strategic development of the Office and the Department's overall privacy program.

C. COMPONENT RESPONSIBILITIES

The establishment of OPCL as a separate office has more clearly defined OPCL's responsibility for management and oversight of the Department's privacy program and components' responsibilities for compliance of component operations. Under the leadership of the CPCLO, components will be responsible for identifying a component privacy official who will be accountable and responsible for the component's privacy program. In the coming year, the CPCLO and OPCL will continue to work with Department leadership to formalize components' responsibilities as they relate to OPCL's mission and the Department's overall privacy program.

D. 2011 ANNUAL REPORT (COVERING 2009-2011)

This report addresses activities between January 2009 and December 2011. Section II (Privacy Policy and Leadership) discusses the activities of the CPCLO, including those related to national security and information sharing, as well as international agreements and activities.

Section III (Privacy Compliance Program) discusses the work of OPCL and how the Department incorporates privacy into its systems, programs, and operations during the development stage. This section also discusses how the Department ensures accountability for its privacy program through reports issued in accordance with the Federal Information Security Management Act of 2002 and Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007.

Section IV (Future Initiatives of DOJ's Privacy Program) provides information about goals and initiatives of the Department's privacy program in 2012 and beyond. As the Department's privacy program matures, the CPCLO and OPCL are committed to continuing their efforts to ensure a strong foundation and culture of privacy throughout the Department.

II. PRIVACY POLICY AND LEADERSHIP -- THE ACTIVITIES OF THE CPCLO

A. STRATEGIC ORGANIZATION OF OPCL

One of the key objectives during this reporting period was to continue the establishment of OPCL as a separate legal office to consolidate the oversight, management, and review of the Department's privacy legal and compliance work. To that end, the CPCLO continued to work with Department leadership to determine the best organizational structure of the Office, its duties and responsibilities, and the relationship of the Office to the privacy officials within the Department components. The work of OPCL is discussed further in Section III of this report.

B. NATIONAL SECURITY

1. National Security Letters

The CPCLO continued the work of the last administration's Acting CPCLO, who led a working group to research and analyze the Federal Bureau of Investigation's (FBI) use of National Security Letters (NSLs). The Working Group was established to respond to the DOJ Inspector General's two reports on NSLs, *A Review of the Federal Bureau of Investigation's Use of National Security Letters* (2007)[4] and *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006* (2008).[5]

The Working Group responded to the Inspector General's recommendations and examined the FBI's use of NSLs to determine whether additional privacy protections were necessary and feasible. The Working Group interviewed analysts, agents, and database managers at FBI Headquarters to discuss how the FBI determines whether information received pursuant to the Electronic Communications Privacy Act is responsive to an NSL request, what they do with information that is non-responsive, how FBI agents determine what information to upload into the database, how agents and analysts access information in the database, and how they determine what information to disseminate. The Working Group also met with FBI employees in several FBI field offices across the country to learn how the analysts and agents used NSLs under existing statutory authorities, Departmental guidelines, and internal FBI policies, as well as how they were incorporating new processes that the FBI had developed to safeguard privacy and civil liberties.

[4] *Available at* http://www.justice.gov/oig/special/s0703b/final.pdf.
[5] *Available at* http://www.justice.gov/oig/special/s0803b/final.pdf.

The CPCLO coordinated and oversaw the completion of new procedures (NSL Procedures) drafted by members of the Working Group and the FBI, and approved by the Attorney General in October 2010. The NSL Procedures reflect a series of measures to improve adherence to the NSL requirements and provide additional privacy safeguards for NSL-derived information without impeding the FBI's operational and technical mission requirements. The CPCLO and the FBI's General Counsel briefed congressional staff on the NSL Procedures in 2010.

2. National Security Reviews

In order to ensure FBI field offices are complying with certain laws, regulations, and policies governing the conduct of national security investigations, including the use of NSLs and the protection of U.S. person information, attorneys from the National Security Division (NSD) and the FBI National Security Law Branch (NSLB) regularly conduct onsite reviews (National Security Reviews or NSRs) of FBI field offices throughout the country. NSD and NSLB attorneys review information and documentation in national security investigative files to ensure FBI agents had the proper predication for opening investigations, obtained necessary authorizations to open investigations and gather information, and complied with relevant statutory and regulatory requirements, as well as the NSL Procedures and applicable Attorney General Guidelines.

The CPCLO receives the NSR reports, which include findings and conclusions from the audits. The CPCLO reviews these reports to ensure both that FBI field offices are in compliance with laws, policies, and procedures designed to protect privacy and civil liberties and that the NSRs are conducted appropriately.

C. INFORMATION SHARING

1. Information Sharing Environment (ISE)

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), established an information sharing environment to facilitate the sharing of terrorism-related information while protecting the privacy and civil liberties of individuals.[6] To that end, the President approved for issuance in 2006 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

[6] *See* 6 U.S.C. § 485(b) (2006).

Guidelines), which require all relevant entities to have a written privacy protection policy that is "at least as comprehensive" as the ISE Privacy Guidelines.[7]

The CPCLO worked with the Office of the Director of National Intelligence's (ODNI) Program Manager for the Information Sharing Environment (PM-ISE) to develop a privacy policy for the Department that met the standards of the ISE Privacy Guidelines. In February 2010, the Deputy Attorney General issued a memorandum for heads of Department components directing them to implement this policy, the *Department of Justice Privacy, Civil Rights, and Civil Liberties Protection Policy for the Information Sharing Environment* (DOJ ISE Privacy Policy or Policy), which fulfills this requirement for the Department.[8]

The DOJ ISE Privacy Policy will both protect the privacy of individuals and enhance our national security by ensuring the confidence and support necessary for the Department's critical information sharing efforts. It applies to all DOJ components that share terrorism-related information with federal, state, local, and tribal law enforcement entities, private sector entities, or foreign partners.[9] The Policy requires each relevant component to designate an ISE Privacy Official who will be responsible for implementing and ensuring compliance with the Policy in that component.[10] The Policy covers "terrorism-related information" that is also "protected information."[11] The ISE Privacy Guidelines define "protected information" 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."[12] Protected information may also include information designated for privacy or other protections by Executive Order, international agreement, or other similar instrument.[13] Under the DOJ ISE Privacy Policy, "terrorism-related information" includes "terrorism information" and "homeland security information," as defined by 6 U.S.C. § 485(a)(5) and 6 U.S.C. § 482(f)(1) respectively, and law enforcement information that is related to terrorism or homeland security and is relevant to a law enforcement mission.[14]

[7] Information Sharing Environment, ISE Privacy Guidelines at 5-6, *available at* http://ise.gov/sites/default/files/PrivacyGuidelines20061204_1.pdf.
[8] Memorandum and DOJ ISE Privacy Policy both attached to this report as Appendix B.
[9] *See* Memorandum at 1.
[10] *See id.*
[11] *See id.* at 2.
[12] Information Sharing Environment, ISE Privacy Guidelines, at 1, *available at* www.ise.gov/sites/default/files/PrivacyGuidelines20061204_1.pdf
[13] *Id.*
[14] *See* Memorandum of DOJ ISE Privacy Policy at 2, attached to this report as Appendix B.

The DOJ ISE Policy applies to all DOJ employees, detailees, contractors, and others who have access to DOJ-protected terrorism-related information.[15] The Policy must also be incorporated into agreements with foreign partners, private partners, and other governmental entities to the extent the agreements involve the sharing of protected terrorism-related information.[16] The CPCLO oversees compliance and implementation of the DOJ ISE Privacy Policy through OPCL and the Component ISE Privacy Officials.

2. Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)

The NSI is a critical part of the federal government's National Strategy for Information Sharing, which articulated a plan to establish a network of state and major urban area fusion centers that could gather and report locally generated information to appropriate federal entities, other states, and localities, while protecting the privacy and legal rights of Americans.[17] The NSI is a partnership for sharing terrorism-related suspicious activity reports (SARs) among federal, state, local, and tribal agencies, including the DOJ Bureau of Justice Assistance in the Office of Justice Programs, the Federal Bureau of Investigation's eGuardian program, the PM-ISE, the Department of Homeland Security, and the Department of Defense. The NSI establishes a national capacity for gathering, documenting, processing, analyzing, and sharing SARs.

On December 17, 2009, the Department was named the Executive Agent to operate the Program Management Office for the NSI, and in March 2010, the Department's Office of Justice Programs established the NSI Program Office, which assists and coordinates the activities and operations of NSI participants. The CPCLO meets regularly with the NSI Program Manager to discuss privacy issues and potential impediments to information sharing.

The CPCLO worked closely with the PM-ISE to develop the NSI Privacy Protection Framework[18] that all sites must implement before participating in the NSI. First, prior to the interstate sharing of SARs, participants must adopt and implement an approved privacy policy that contains ISE-SAR privacy protections that are in compliance with the *ISE-SAR Privacy, Civil Rights, and Civil Liberties Protection Policy Template* or the

[15] *See* Memorandum at 2, attached to this report as Appendix B.
[16] *See id.*
[17] *See* National Strategy for Information Sharing at 11, *available at* http://ise.gov/sites/default/files/nsis_book_0.pdf.
[18] *See* Nationwide SAR Initiative Privacy Fact Sheet NSI Privacy Protection Framework, *available at* http://nsi.ncirc.gov/documents/SAR_Privacy_Fact_Sheet_2012.pdf

Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template.[19]

Second, all participants must adopt the ISE-SAR Functional Standard v. 1.5,[20] which is designed to ensure the protection of constitutional rights, including the protection of rights guaranteed by the First Amendment and limitations on the use of certain factors – including race, ethnicity, national origin, or religious affiliation – in the gathering, collecting, storing, and sharing of information about individuals. In order to meet the Functional Standard, a SAR must be based on observed behavior and not on ethnicity, race, national origin, or religious affiliation. Specifically, it defines "suspicious activity" as "observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity."[21] Supervisors and trained analysts must review all SARs received (from law enforcement officers, private sector partners, etc.) to determine whether they have a potential nexus to terrorism and whether they describe one of the behaviors identified by the Functional Standard.[22] The Functional Standard also includes reliability indicators developed with the help of privacy advocates.

Third, all NSI sites are required to provide relevant personnel with privacy training, which covers the ISE-SAR Functional Standard v. 1.5, as well as other privacy, civil rights, and civil liberties issues.[23]

The CPCLO participated as a panelist at the National Fusion Center Conferences in February 2010 and March 2011, where she discussed the importance of ensuring privacy and civil liberties protections in the Nationwide SAR Initiative.

3. Interagency Threat Assessment and Coordination Group (ITACG)

The *Implementing Recommendations of the 9/11 Commission Act of 2007* (9/11 Commission Act) formally established the Interagency Threat Assessment and Coordination Group (ITACG) to improve the sharing of information within the ISE.[24] The ITACG is comprised of an ITACG Detail and an ITACG Advisory Council. Both

---

[19] *See id.; see also* Information Sharing Environment, Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Template (2010), *available at* http://ise.gov/sites/default/files/Fusion%20Center%20Privacy%20Policy%20Development_508compliant.pdf.

[20] A*vailable at* http://ise.gov/sites/default/files/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf

[21] *Id.* at 2.

[22] *Id.* at 8-10.

[23] *See* Nationwide SAR Initiative Privacy Fact Sheet NSI Privacy Protection Framework, *available at* http://nsi.ncirc.gov/documents/SAR_Privacy_Fact_Sheet_2012.pdf.

[24] *See* Homeland Security Act § 210D, 6 U.S.C. § 124k (2006), amended by Implementing Recommedations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 521, 121 Stat. 266 (2007).

the Detail and the Council are led by senior federal law enforcement and intelligence personnel but consist primarily of representatives from state and local government. The ITACG improves information sharing between the Intelligence Community (IC) and state and local governments by recommending and facilitating the dissemination of national intelligence products that may be of use to state and local government officials.

The 9/11 Commission Act requires the Department's CPCLO and the Department of Homeland Security Officer for Civil Rights and Civil Liberties, in consultation with the Civil Liberties Protection Officer of the Office of the Director of National Intelligence, to submit reports assessing the privacy and civil liberties impact of the ITACG.[25] A privacy impact assessment concerning the ITACG was prepared in July 2008. A civil liberties impact assessment concerning the ITACG was prepared and submitted to Congress in September 2010. The 2010 Report on the ITACG found that the civil liberties impact assessment identified potential civil liberties risks and found that existing training, supervision, and oversight of ITACG activities are sufficient to mitigate those risks.[26] To ensure that civil liberties are protected, the report nevertheless recommended that the ITACG Advisory Council augment its policies governing the ITACG Detail.[27] Specifically, the report recommended including guidance on access to and dissemination of information, as well as guidance on the use of race, ethnicity, religion, and other sensitive classifications.[28] Compliance with this clear, written guidance should prevent inappropriate or unlawful dissemination of information or use of inappropriate vetting criteria and should reinforce the proper application of the National Counterterrorism Center's existing operational policies to ITACG activities.

D. INTERNATIONAL ACTIVITIES

The CPCLO has worked extensively with the United States government's international partners on data protection agreements to facilitate information sharing for law enforcement and counterterrorism purposes.

1. High Level Contact Group

In November 2006, the United States (U.S.)-European Union (EU) Justice and Home Affairs Ministerial Troika established a High Level Contact Group (HLCG) to discuss privacy and personal data protection in the context of the exchange of information for law enforcement purposes. The protection of personal data was, and continues to be, the

[25] *Id.* 121 Stat. at 332.
[26] *See* 2010 Report on the Interagency Threat Assessment and Coordination Group (ITACG) at 14, *available at* http://ise.gov/sites/default/files/2010_ITACG_Report_Final_30Nov10.pdf.
[27] *See id.* at 14.
[28] *See id.*

most difficult issue in the U.S. government's information sharing negotiations with the EU and its Member States.

The CPCLO served as the Department's representative to the U.S.-EU HLCG, which also included representatives from the Department's Office of International Affairs, the U.S. Departments of Homeland Security and State, the European Commission, and the European Council Presidency (supported by the Council Secretariat). The goal of the HLCG was to resolve disputes and misconceptions about data protection in order to facilitate and improve transatlantic information sharing for law enforcement purposes, including counterterrorism investigations and terrorism prosecutions.

The HLCG convened for numerous meetings in 2009 (both in person and via video teleconference) to educate one another about the U.S. and EU legal frameworks for data protection and to finalize a set of core data protection principles that would serve as a foundation for a future binding data protection agreement.

In October 2009, the HLCG concluded its work and agreed to finalize a statement of data protection principles that would govern law enforcement information sharing between the U.S. and the EU. At the Justice and Home Affairs Ministerial on October 28, 2009, the Attorney General and Swedish Minister of Justice, representing the EU Swedish Presidency, signed a Declaration acknowledging the conclusion of the work of the HLCG and committed the U.S. and the EU to begin negotiations on a binding international data protection agreement embodying those principles.

2. International Multilateral Agreements

In December 2010, the European Commission received its mandate to negotiate a binding international agreement to ensure data protection for both U.S. and EU citizens when information is shared for law enforcement purposes. The CPCLO and representatives from the DOJ's Criminal Division's Office of International Affairs and from the Departments of Homeland Security and State began negotiations for a binding Data Privacy and Protection Agreement (DPPA) with a delegation from the European Commission in March 2011. The negotiating teams have met numerous times over the last year and negotiations are ongoing.

The CPCLO also was a member of the U.S. team that negotiated the U.S.-EU Passenger Name Record (PNR) Agreement. (The U.S. Team included other officials from DOJ, the Department of Homeland Security, and the State Department.) The new agreement will build on the existing PNR Agreement that has been in effect since 2007 and will protect national security and public safety while respecting the privacy of airline passengers. The U.S.-EU PNR Teams held their inaugural meeting on December 8, 2010, and negotiations concluded in November 2011, when an agreement was initialed by officials

from the U.S. and the EU. In February 2011, the CPCLO participated as a member of the Terrorist Finance Tracking Program (TFTP) Agreement Review Team. The TFTP Agreement between the Treasury Department and the EU was signed in 2010 and allows the transfer of financial data from the EU to Treasury for counterterrorism purposes. The TFTP Agreement provides privacy protections for the data transferred and requires an annual audit of the program's compliance with these protections. The EU delegation that participated in the audit deemed it a success.

3. International Bilateral Agreements

In addition to participating in negotiations with the EU, the CPCLO has also worked with the Department's Office of International Affairs and representatives from the Department of Homeland Security to negotiate agreements with two European countries (Austria and Belgium) to share fingerprint data for law enforcement purposes. These Preventing and Combating Serious Crime (PCSC) agreements establish processes to conduct fingerprint matching, procedures to allow additional sharing of data in the event of a match, redress procedures for individuals whose information is shared, and other data protection provisions. The PCSC agreements are modeled after the European convention known as the Prüm Treaty, which provides strong data protection by limiting access to individual fingerprints on a hit/no-hit basis. If the fingerprint data queried against the data base does not register a "hit," no other data is exchanged. The information can only be used for a criminal justice purpose, as defined by 28 C.F.R. § 20.3(b), and fingerprints can only be used if collected from the individual about whom information is sought.

The CPCLO also serves as the U.S. co-lead (with the DHS Chief Privacy Officer) of the working group charged with developing a set of privacy principles to inform and guide information sharing between U.S. and Canadian government agencies under the Beyond the Borders Declaration signed in 2011 by President Obama and Canadian Prime Minister Harper.

E. OTHER LEADERSHIP ACTIVITIES

The CPCLO conducts privacy policy reviews that affect the DOJ's mission on a department-wide level and actively participates in many intra- and inter-agency groups to ensure a coordinated and uniform approach to privacy policy across the Department and the federal government.

1. Intra-Agency Leadership Activities

a. Data incidents and breach responses

The Identity Theft Task Force's memorandum, *Identity Theft Related Data Security Breach Notification Guidance* (9/19/2006), and OMB's M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (5/22/2007), required agencies to create data breach procedures and a response team to respond to data breaches involving personally identifiable information (PII).[29] The Department drafted the "Incident Response Procedures for Data Breaches Involving Personally Identifiable Information" (Incident Response Procedures) and established a Core Management Team (CMT), which is co-chaired by the CPCLO and the Department's Chief Information Officer. [30] Under the Incident Response Procedures, when a possible breach of PII occurs of a certain risk level, the Office of the Chief Information Officer (OCIO) notifies the CPCLO and OPCL.[31] The CPCLO, OPCL, and OCIO decide whether the CMT should meet to discuss a particular incident or whether the incident can be managed without a meeting. The CMT is comprised of representatives from all of the Department's leadership components. It meets to conduct a risk assessment and develop a response to the breach, as well as policies and procedures that the Department could adopt to prevent future breaches.

b. Computer Matching Agreements

The CPCLO is also a key member of the Department's Data Integrity Board. The Data Integrity Board oversees and coordinates the implementation of the Computer Matching Act by conducting reviews and approvals of computer matching agreements entered into by Department components, and by providing interpretations and guidance to Department components in the conduct of matching agreements. During this reporting period, the Data Integrity Board considered and approved six computer matching agreements.

2. Interagency Leadership Activities

a. Federal CIO Council Privacy Committee

From June 2009 until November 2011, the CPCLO was a co-chair of the Federal Chief Information Officers Council Privacy Committee, along with the Chief Privacy Officer of

[29] *See* http://m.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2006/task_force_theft_memo.pdf and http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.
[30] *See* http://www.justice.gov/opcl/breach-procedures.pdf.
[31] *See id.* at 8-9.

the Department of Homeland Security and the Assistant Secretary for Information and Technology at the Department of Veterans Affairs.

The Privacy Committee serves as the interagency coordination committee for Senior Agency Officials for Privacy in the federal government. It provides a forum for the development of privacy policies and promotes practices to create a culture of privacy. The Privacy Committee makes policy recommendations to federal government agencies to ensure adherence to the letter and spirit of the privacy laws applicable to U.S. government agencies, including the Privacy Act of 1974 and the E-Government Act of 2002, as well as the widely accepted fair information practice principles.

The Privacy Committee supports the following four subcommittees: the International Subcommittee, which promotes an understanding of international data protection frameworks, assists in the coordination of requests for information by foreign governments about the U.S. data protection framework, and supports efforts to ensure a consistent message on privacy from U.S. government agencies; the Best Practices Subcommittee, which identifies agencies' best practices for federal privacy programs and makes recommendations to the Committee on how agencies can improve the implementation of privacy laws, regulations, and policies; the Development and Education Subcommittee, which educates federal employees about privacy laws, regulations, and policies through educational materials and the annual Privacy Summit; and the Web 2.0 Subcommittee, which developed recommendations for federal agencies on how to promote President Obama's Open Government initiative (including agencies' use of social media tools) while ensuring appropriate privacy protections for personally identifiable information.

b. Privacy and Civil Liberties Sub-Interagency Policy Committee (Sub-IPC) of the Information Sharing and Access IPC

The CPCLO also serves on the Executive Committee of the Privacy and Civil Liberties (PCL) Sub-IPC, along with the Chief Privacy Officer of the Department of Homeland Security and the Civil Liberties Protection Officer of the Office of the Director of National Intelligence. (The PM-ISE Privacy Guidelines Committee, which had worked for several years on privacy guidelines for terrorism-related information sharing in the Information Sharing Environment, was reconstituted in 2010 as the PCL Sub-IPC.) The PCL Sub-IPC meets regularly to ensure that federal agencies adopt, implement, and enforce privacy and civil liberties protection policies before sharing terrorism-related information in the ISE.

c. National Science and Technology Council Subcommittee on Privacy and Internet Policy (Office of Science and Technology Policy)

The CPCLO is also a member of the National Science and Technology Council's Subcommittee on Privacy and Internet Policy, an interagency group that provides strategic direction on information privacy policy and seeks to find legislative, regulatory, and international policy consensus. The Subcommittee will consider and encourage the development of best practices for information architecture, data management, and overall privacy policy frameworks.

F. PRIVACY DISCUSSIONS

The CPCLO has hosted multiple meetings with privacy advocates to discuss the Department's protection of privacy and civil liberties. In addition, the CPCLO has participated in panel discussions hosted by and for privacy advocates to discuss the Department's use of its surveillance authorities and to ensure an ongoing dialogue between the Department and the privacy community.

In addition, to increase the Europeans' understanding of the U.S. privacy framework and to identify common core data protection principles, the CPCLO has participated in panel discussions and press availabilities with European governmental institutions, think tanks, and media outlets and meets frequently with foreign government officials to discuss data privacy under U.S. law.

III. PRIVACY COMPLIANCE PROGRAM – THE ACTIVITIES OF OPCL

The CPCLO has charged OPCL with primary responsibility to ensure the Department's compliance with federal privacy laws and Administration and Department privacy policies by providing legal and policy guidance, fulfilling administrative law requirements, and developing and providing training in connection with the Privacy Act of 1974 and the privacy provisions of the E-Government Act of 2002 and the Federal Information Security Management Act of 2002 (FISMA). This section discusses OPCL's activities during this reporting period.

A. INITIAL PRIVACY ASSESSMENTS (IPAs)

The Department's collection and use of information about individuals is critical to its ability to effectively enforce the law, defend the interests of the United States, and ensure public safety. As it fulfills this mission, the Department must also fulfill its responsibility to manage and protect the personally identifiable information it collects. The balance between the government's need to maintain information about individuals and the individual's right to be protected from unwarranted invasions of personal privacy is at the

core of the federal privacy laws that OPCL administers as part of the Department's privacy compliance program.

The privacy compliance process begins when the Department first determines it needs to collect personally identifiable information. In 2009, OPCL established a new process – called the Initial Privacy Assessment (IPA) – to make the Department's compliance with federal privacy laws and regulations at this early stage more effective and efficient. The IPA allows the Department's components to streamline the assessment of information privacy issues associated with systems and programs that involve the collection and storage of personally identifiable information. It operates as a tool to facilitate the identification of potential privacy issues; assess whether additional privacy documentation is required, such as creation or modification of a Privacy Act system of records notice (SORN) or a Privacy Impact Assessment (PIA); and ultimately, to ensure the Department's compliance with applicable privacy laws and policies.

The IPA consolidates the various statutory privacy compliance requirements into a single, unified, and comprehensive process. It also bridges the IT security and privacy processes and communities. The Department has incorporated the IPA process into its IT security documentation and the software application used to track compliance of electronic systems with the FISMA. IPAs are mandated as part of the certification and accreditation (C&A) process, which requires the program managers for IT systems, either in development or operation, to evaluate security controls to ensure that security risks have been properly identified and mitigated. The inclusion of the IPA in this process assists in identifying information assets requiring appropriate security controls and permits better identification of those systems containing and maintaining personally identifiable information. Through the IPA, components can identify steps to mitigate any potential adverse impact on privacy at the outset of the information collection or program. For example, a component may determine that the collection and use of Social Security Numbers (SSNs) within a system is not necessary. The component can then forgo the collection of SSNs in accordance with privacy protection directives and policies issued by the Office of Management and Budget (OMB). (In 2010 and 2011, OPCL reviewed and made determinations on a total of 144 IPAs submitted by Department components.)

In March 2010, OPCL updated and revised the IPA template and instructions.[32] These documents will evolve as the Department's IT and privacy officials work together to find better solutions for privacy compliance. That same year, OPCL began providing internal training on this new process and has continued this training on an ongoing basis.

[32] The new IPA template is available at http://www.justice.gov/opcl/initial-privacy-assessment.pdf.

B. SORNS, ACCOMPANYING EXEMPTION REGULATIONS, AND COLLECTION NOTICES

Under the Privacy Act of 1974, agencies must assess their handling of information about individuals and ensure the collection, maintenance, use, disclosure, and safeguarding of such information is appropriate and legal.[33] As part of this compliance process, agencies must review each system of records that contains such information and document and describe the proper maintenance and handling of such information in a system of records notice (SORN). A SORN provides the public with details about a system of records, including its purpose, the categories of individuals affected by its operations, the categories of information to be used and collected by the agency, where the agency maintains the information, what means of access and correction are available to the individual, what security safeguards protect the information, and with whom and under what conditions the agency will share the information in the system.[34] The Department of Justice maintains approximately 200 systems of records. The SORNs for these systems can be found on the Department of Justice's website at www.justice.gov/opcl/privacyact.html.

Through the IPA process, OPCL advises the Department's components on the proper maintenance of information in systems of records in order to ensure compliance with the numerous statutory requirements that govern such information. Once it is determined that the Department maintains a system of records, components draft the SORNs and any accompanying exemption regulation, if appropriate. OPCL reviews all such SORNs and accompanying exemption regulations for approval and issuance by the CPCLO.[35] For example, OPCL assists components in developing appropriate language for SORNs and reviews routine uses included in SORNs to ensure that each disclosure of information is compatible with the purpose for which the information is collected. OPCL also reviews any accompanying exemption regulation to ensure that exemptions are legally sufficient and appropriate. During the 2009-2011 reporting period, the Department published ten new or modified SORNs. In addition to SORNs, OPCL advises components on preparing other Privacy Act compliance documents, such as Privacy Act statements, which provide notice to the individual concerning an agency's collection authority and the possible uses of information collected about individuals.[36]

[33] *See* 5 U.S.C. § 552a (2006).
[34] *See id.* § 552a(e)(4).
[35] The Attorney General delegated his authority to carry out these responsibilities to the CPCLO by order in January 2008.
[36] *See* 5 U.S.C. § 552a(e)(3).

C. PRIVACY IMPACT ASSESSMENTS (PIAs)

Section 208 of the E-Government Act of 2002 requires all federal agencies to conduct a PIA in certain circumstances before developing or procuring information technology that collects, maintains, or disseminates information in identifiable form or before initiating a new collection of such information that will be collected, maintained, or disseminated using information technology.[37] PIAs provide an analysis of how information is handled to ensure compliance with applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of collecting, maintaining, and disseminating such information in an electronic information system; and to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[38]

Through the IPA process, OPCL serves as the focal center for the PIA process in the Department. OPCL provides guidance and training to components on compliance with the E-Government Act privacy requirements; reviews PIAs in preparation for signature by the CPCLO; and provides public notice of PIAs, as appropriate.[39] OPCL also drafts PIAs that cover the Department's information systems, such as the PIA mentioned below concerning social media uses in the Department. The Department's components, however, are primarily responsible for preparing PIAs and must ensure a collaborative effort among the component privacy official, program officials, and the information technology experts. After all privacy concerns have been fully addressed and after review by the Department's CIO, the PIA is presented to the CPCLO for approval with the recommendations of the CIO and OPCL. In August 2010, OPCL developed a new PIA template for components to use.[40] During the 2009-2011 reporting period, the CPCLO approved 30 PIAs, and all non-national security system DOJ PIAs can be found on the Department's website at www.justice.gov/opcl/pia.htm.

In conducting a PIA analysis, the Department considers the privacy impacts from the beginning of a system's development through the system's life cycle to ensure that system developers and owners have made technology choices that incorporate privacy protections into the underlying architecture of the system. As with the IPA, PIAs have been incorporated in the DOJ IT security framework, which ensures the identification of all information technology systems that require PIAs and allows OPCL and OCIO to resolve all privacy and related security issues before a system is certified and accredited.

---

[37] *See* E-Government Act of 2002 § 208, 44 U.S.C. § 3501 (note) (2006).
[38] *See id.*
[39] In March 2007, Department Order 3011 was modified to reflect the transition of responsibility for approval of PIAs to the CPCLO. The current order is DOJ 3011.1A.
[40] The new PIA template, which was modified slightly in March 2012, is available at http://www.justice.gov/opcl/docs/doj-pia-template-march2012.pdf.

D. LEGAL GUIDANCE AND TRAINING

OPCL serves as the primary legal counsel for the Department on federal information privacy requirements, policies, and initiatives. In this capacity, OPCL advises components about the applicability and requirements of the Privacy Act, as interpreted in case law and OMB guidance, to help Department components protect the privacy rights of individuals as they perform their agency operations and functions. In addition, OPCL advises Department components on Privacy Act issues that arise in connection with litigation and legislative proposals; develops and conducts Privacy Act training; and provides guidance on Privacy Act regulations. OPCL also has provided substantial comments on pending legislation, Congressional testimony, Executive Orders, reports and other policy matters concerning Privacy Act compliance and related issues.

In 2010, OPCL prepared and issued a new, revised edition of the *Overview of the Privacy Act of 1974* (*Overview*).[41] This is a biennial publication, which provides a thorough and up-to-date legal analysis of the Privacy Act's agency record-keeping requirements, disclosure prohibition, and access and amendment provisions, and provides a reference to, and legal analysis of, court decisions interpreting the Privacy Act's provisions. The *Overview* is a valued resource and is widely used throughout the federal government for guidance in this field. As stated above, OPCL will publish its 2012 edition of the *Overview* later this year.

OPCL must rely on the privacy and security personnel in the Department's components to alert it of any privacy issues of which they become aware. For this reason, OPCL conducts a comprehensive and robust training program to ensure that appropriate personnel are well trained to spot issues, resolve problems, and ensure compliance with privacy laws and policies. During this reporting period, OPCL has provided privacy training on:

- the new IPA and PIA processes to Department privacy and security personnel;
- the SORN drafting process to the Department's component privacy officials and IT experts who are directly responsible for IPAs and PIAs;
- general Privacy Act compliance as part of the Department's Office of Legal Education training program to a broader cadre of Department and other agency personnel on an annual basis; and
- various other privacy training including workshops on the interface between the privacy provisions of the E-Government Act and the Privacy Act; the interface

[41] An electronic version of the *Overview* is available at www.justice.gov/opcl/1974privacyact-overview.htm.

between the Freedom of Information Act and the Privacy Act; litigation concerns involving the Privacy Act; and law enforcement records and the Privacy Act.

Training for fiscal year 2012 can be located on the Department's website at www.justice.gov/usao/eousa/ole. OPCL also revised the privacy awareness sections of the Department's Computer Security Awareness Training, which is required training for every Department employee. Lastly, OPCL also provides training at, and participated in, other programs, including the International Association of Privacy Professionals conferences, the CIO Council Privacy Committee Privacy Summit, and other agency conferences that addressed information privacy issues.

E. ACCOUNTABILITY AND REPORTING

OPCL is responsible for issuing quarterly reports as required by Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (803 Reports) and for coordinating the senior agency official for privacy sections of the quarterly and annual reports in accordance with the FISMA.

1. FISMA Audits - Office of the Inspector General

In accordance with the FISMA, the Department's Office of the Inspector General (OIG) performs an independent evaluation of the Department's information security program and completes an OMB reporting template. As part of this evaluation, the auditors assess the Department's overall privacy program and its implementation at the component level. OPCL works with the Department's components that are subject to audit to respond to the privacy compliance questions. OPCL also coordinates any remedial action for the Department's privacy program that is required as a result of the OIG audit.

In 2011, the OIG conducted an assessment of the Department's overall privacy program, and it recommended that OPCL work towards more clearly identifying and documenting the privacy roles and responsibilities of OPCL and the Department components, and that a senior component official for privacy should be established at each DOJ component. To that end, OPCL has worked with the CPCLO and other Department leadership to draft a Department order that would establish these roles and responsibilities in order to fully respond to the OIG's recommendations.

2. FISMA Reporting Requirements

Federal agencies are also required to submit annual and quarterly reports to OMB regarding their privacy programs in accordance with the FISMA and OMB guidance

implementing the FISMA.[42] The CPCLO and OPCL are responsible for preparing these FISMA privacy reports for OMB on behalf of DOJ. The quarterly reports reflect the information provided in the Department's IPAs and help OPCL to determine the number of information systems in the Department that collect personally identifiable information, require PIA and Privacy Act documentation, and have completed such documentation. The annual report includes the information collected quarterly and also requires the CPCLO and OPCL to collect data and report on the Department's privacy program. To aid in the collection of this information, OPCL worked with OCIO to develop the capability within the software application that tracks FISMA compliance to capture relevant privacy information and documentation. OPCL also helped test the Cyberscope application that is now used by OMB to collect all agencies' quarterly and annual FISMA report data.

In FY 2009, OPCL reviewed Department OMB 300 submissions for privacy issues; however, in FY 2010, OMB removed privacy questions from these submissions. OPCL therefore no longer conducts this review.

3. Section 803: Privacy and Civil Liberties Complaints

As mentioned above, OPCL submits 803 Reports to Congress on a quarterly basis. These 803 Reports provide information related to the fulfillment of certain privacy and civil liberties functions of the CPCLO, including information on the number and types of reviews undertaken; the type of advice provided and the response given to such advice; the number and nature of the complaints received by the Department, agency, or element concerned for alleged violations; and a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of the CPCLO. Many of these duties are discharged by OPCL on behalf of the CPCLO. The quarterly reports issued by OPCL during the 2009-2011 reporting period may be found on the Department's website at www.justice.gov/opcl/reports.htm.

F. PARTICIPATION IN INTRA-AGENCY COMMITTEES

OPCL participates on many different intra-agency committees to provide privacy legal and compliance guidance, including the Core Management Team (CMT), which handles data breaches, and the Department's Web 2.0 Working Group.

[42] *See* 44 U.S.C. § 3544(c) (2006); *see also* http://www.whitehouse.gov/omb/inforeg_infopoltech#pg for annual OMB FISMA guidance.

1. Data Breach Response

As discussed above, OPCL participates in the Department's review of incidents and data breaches pursuant to the Department's Incident Response Procedures.[43] The Incident Response Procedures established a CMT which is co-chaired by the CPCLO and the Department's CIO. The CPCLO and OPCL are notified of possible breaches of PII, and in conjunction with the OCIO, decide whether the CMT should meet to discuss a particular incident. OPCL provides legal guidance to the CMT regarding the privacy implications associated with data breach incidents and the Department's response.

2. Open Government Initiatives

Technological advances have revolutionized the way in which information is distributed between and among individuals and has facilitated the development of new communications technologies. As part of the Obama Administration's initiative to make the federal government more transparent, participatory, and collaborative, as set forth in the President's January 21, 2009, Memorandum on Transparency and Open Government (Open Government Initiative),[44] the Department and other federal agencies have adopted new social media tools to communicate and interact with the public. In December 2009, OMB issued new policies governing the implementation of the President's Open Government initiative.[45] OPCL has worked with OMB, the CIO Council, and with Department components to address privacy issues, including legal compliance, associated with the use of these emerging technologies.

After the President announced the Open Government initiative, the CPCLO and OPCL and the Department's Web 2.0 Policy Working Group began addressing the Department's use of new media. The Department's Office of Public Affairs (OPA) completed the *Privacy Impact Assessment for Third-Party Social Web Services*, issued on September 28, 2009.[46] The Department, through the Web 2.0 Policy Working Group, determined that privacy would be adequately protected as long as certain processes were followed. Specifically, the Department established a business process that (i) gave OPA responsibility for ensuring the propriety of the Department's business use of the third-party websites and (ii) required the Department's Web 2.0 Policy Working Group to review applications for use of the third-party websites to ensure compliance with applicable laws, policies and regulations.[47] Further, the Department determined that

[43] *See* http://www.justice.gov/opcl/breach-procedures.pdf.
[44] *Available at* www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment.
[45] *See* http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf.
[46] An electronic version of this PIA is available at http://www.justice.gov/opcl/docs/opa-webservices-pia.pdf.
[47] *See id.* at 2.

"[b]ecause the accounts that the Department will open on these third-party websites are not a part of the Department's internal information systems nor will they be operated by a contractor of the Department, the Department does not and will not collect information from individuals when individuals interact with the Department's social web accounts."[48] OPCL is an active member of the Web 2.0 Policy Working Group, and, if OPA approves a request, the component is required to send an initial privacy assessment to OPCL for review.

On June 25, 2010, OMB issued a memorandum (M-10-23) to provide privacy guidance to federal agencies using "third-party websites and applications."[49] This memorandum requires agencies to prepare an "adapted PIA" whenever "an agency's use of a third-party website or application makes PII available to the agency."[50] OPCL is implementing these requirements and will modify its guidance to Department components, as appropriate. OPCL will remain engaged in new media issues to ensure the protection of privacy interests and compliance with privacy requirements.

IV. FUTURE INITIATIVES OF THE DOJ PRIVACY PROGRAM

The CPCLO and OPCL are committed to building a strong foundation of privacy at the Department and will continue to build upon the initiatives discussed in this report. To that end, the CPCLO and OPCL will continue the work of establishing and strengthening the Department's components' roles and responsibilities in order to build a successful and accountable privacy program. This year, OPCL will also publish the 2012 edition of the *Overview of the Privacy Act of 1974*. Finally, recognizing the rapid pace of technological advancement, the Department will continue to work closely with the Department's OCIO and its IT professionals to ensure that privacy principles are considered and privacy legal and policy requirements are met as the Department uses new technologies. As the privacy and security communities work more closely together, the Department hopes to discover even better solutions to enhance privacy safeguards for the information that it maintains. The Department looks forward to discussing these new initiatives in the next annual report.

[48] *Id.*
[49] *Available at* http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf.
[50] *See id.* at 4.

Appendix A. List of Key Laws and Regulations Applicable to Department of Justice Privacy Activities:

- Department of Justice regulations at 28 CFR Part 16. Subpart D. Protection of Privacy and Access to Individual Records under the Privacy Act of 1974
- E-Government Act of 2002 § 208, 42 U.S.C. § 3501 (note) (2006)
- Federal Information Security Management Act of 2002, 44 U.S.C. § 3541 *et seq.* (2006)
- Implementing Recommendations of the 9/11 Commission Act of 2007 § 803, 42 U.S.C. § 2000ee-1 (2006)
- Intelligence Reform and Terrorism Prevention Act of 2004, 6 U.S.C. § 485 (2006)
- Privacy Act of 1974, 5 U.S.C. § 552a (2006)
- Violence Against Women and Department of Justice Reauthorization Act of 2005 § 1174, 28 U.S.C. § 509 (note) (2006)

Appendix B

U.S. Department of Justice

Office of the Deputy Attorney General

The Deputy Attorney General

Washington, D.C. 20530

February 3, 2010

MEMORANDUM FOR HEADS OF DEPARTMENT COMPONENTS

FROM: David W. Ogden
Deputy Attorney General

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

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007, established an information sharing environment (ISE) to facilitate the sharing of terrorism-related information while protecting the privacy, civil rights, and civil liberties of individuals.[1] To that end, the President approved for issuance 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), which require all relevant entities to have a written privacy protection policy that is "at least as comprehensive" as the ISE Privacy Guidelines.[2]

Relevant Components' implementation of the attached *Department of Justice Privacy, Civil Rights, and Civil Liberties Protection Policy for the Information Sharing Environment* (DOJ ISE Privacy Policy or Policy) will fulfill this requirement for DOJ. The Policy will also be available at www.justice.gov.

The DOJ ISE Privacy Policy will apply to all DOJ Components that share terrorism-related information with federal, state, local, and tribal law enforcement entities, private sector entities, or foreign partners. The Policy requires each relevant Component to designate an ISE Privacy Official who will be responsible for implementing the Policy in that Component.

[1] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1016(b)(1), 18 Stat. 3665 (Dec. 17, 2004).

[2] *See* An Introduction to the ISE Privacy Guidelines (Dec. 4, 2006), *available at* http://www.ise.gov/docs/privacy/ISEPrivacyGuidelinesIntroduction.pdf; *see also* Memorandum from the President to the Heads of Executive Departments and Agencies on the Guidelines and Requirements in Support of the Information Sharing Environment (Dec. 16, 2005) (requiring the head of each executive department that possesses or uses intelligence or terrorism information to ensure that the department fully implements privacy guidelines approved by the President).

The Policy will apply immediately to Components that are participating in the Nationwide Suspicious Activity Reporting Initiative and sharing terrorism-related Suspicious Activity Reports through the FBI's eGuardian system. All other relevant Components must implement the Policy by April 30, 2010.

The Policy only covers terrorism-related information that is also "protected information." The ISE Privacy Guidelines define "protected information" 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."[3] Protected information may also include information designated for privacy or other protections by Executive Order, international agreement, or other similar instrument.

"Terrorism-related information" includes "terrorism information" and "homeland security information," as defined by IRTPA § 1016(a)(4) and 6 U.S.C. 482(f)(1) respectively, and law enforcement information that is related to terrorism or homeland security and is relevant to a law enforcement mission. (Appendix A of the Policy defines all relevant terms.)

The Policy applies to all DOJ employees, detailees, contractors, and others who have access to DOJ protected terrorism-related information. The Policy must also be incorporated into agreements with foreign partners, private partners, and other governmental entities to the extent the agreements involve the sharing of protected terrorism-related information.

This Policy will both protect the privacy of individuals and enhance our national security by ensuring the confidence and support necessary to the Department's critical information sharing efforts.

Questions about the DOJ ISE Privacy Policy should be directed to Nancy Libin, Chief Privacy and Civil Liberties Officer, at (202) 307-0697 or Nancy.C.Libin@usdoj.gov.

[3] *See* ISE Privacy Guidelines at 1, *available at* www.ise.gov/docs/privacy/PrivacyGuidelines20061204.pdf

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