U.S. Department of Justice

THE CHIEF PRIVACY AND CIVIL LIBERTIES OFFICER AND THE OFFICE OF PRIVACY AND CIVIL LIBERTIES

ANNUAL PRIVACY REPORT

JANUARY 1, 2012-SEPTEMBER 30, 2013

United States Department of Justice
Annual Privacy Report

Message from the Acting Chief Privacy and Civil Liberties Officer

I am pleased to present the Department of Justice's (Department or DOJ) Annual Privacy 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 the Violence Against Women and Department of Justice Reauthorization Act of 2005. This report covers the period from January 1, 2012, through September 30, 2013, and includes the achievements of the prior CPCLO, Nancy C. Libin, who served as the Department's CPCLO from June 2009 through August 2012.

The Department's privacy program is supported by a team of dedicated privacy professionals who strive to build a culture and understanding of privacy within the complex and diverse mission work of the Department. The work of the Department's privacy team is evident in the care, consideration, and dialogue about privacy that is incorporated in the daily operations of the Department.

As a member of the Department's privacy team, I am committed to developing innovative, practical, and efficient ways to incorporate and implement privacy requirements and principles as the Department carries out its important mission of protecting and serving the American public.

Joo Y. Chung
Acting Chief Privacy and Civil Liberties Officer
U.S. Department of Justice

Table of Contents

LEGISLATIVE LANGUAGE

This report has been prepared in accordance with Section 1174 of the Violence Against Women and Department of Justice Reauthorization Act of 2005,[1] which states:

28 U.S.C. 509, Section 1174. Privacy Officer

> Annual Report -- The privacy official shall submit a report to the Committees on the Judiciary of the House of Representatives and of the Senate on an annual basis on activities of the Department that affect privacy, including a summary of complaints of privacy violations, implementation of section 555a of title 5, United States Code, internal controls, and other relevant matters.

[1] 28 U.S.C. § 509 (note) (2012).

BACKGROUND

1. 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, use, maintenance, and disclosure of personally identifiable information (PII). The CPCLO also advises the head of the Department on privacy issues when the Department proposes, develops, or implements laws, regulations, policies, procedures, or guidelines related to its counterterrorism efforts.[2] Additionally, the CPCLO is responsible for advising the head of the Department 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)."[3]

2. THE OFFICE OF PRIVACY AND CIVIL LIBERTIES

The Office of Privacy and Civil Liberties (OPCL) was created as a separate office in 2008 to support the work of the CPCLO, consolidate the Department's privacy compliance and legal work, and provide consistency and leadership to all Department components on information privacy issues. The Director of OPCL reports directly to the CPCLO in ODAG, and the Office is currently comprised of seven employees, who include the Director, four staff attorneys, one privacy analyst, and one program specialist. Each OPCL staff attorney works with a defined set of Department components, and also specializes in certain subject areas of federal information privacy law.

OPCL supports the CPCLO's statutory duties by implementing and coordinating the Department's privacy compliance and legal program. OPCL's principal mission is to ensure that the Department complies with federal information privacy laws, regulations, policies, and other authorities in all of 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;

[2] *See* Violence Against Women and Department of Justice Reauthorization Act of 2005 § 1174, 28 U.S.C. § 509 (note) (2012); *see also* Implementing Recommendations of the 9/11 Commission Act of 2007 § 803, 42 U.S.C. § 2000ee-1 (2012).
[3] Violence Against Women and Department of Justice Reauthorization Act of 2005 § 1174, 28 U.S.C. § 509 (note) (2012).

- Reviewing legislative proposals pertaining to privacy issues that impact the Department's handling of information;
- Adjudicating appeals of denials by DOJ components to amend records under the Privacy Act;
- Establishing and providing annual and specialized privacy compliance, legal, and awareness training to Department personnel;
- Ensuring adequate procedures for responding to privacy and civil liberties inquiries and complaints from the public;
- Preparing and/or coordinating the 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 (FISMA) of 2002, Section 1174 of the Violence Against Women and Department of Justice Reauthorization Act of 2005, and the Federal Agency Data Mining Reporting Act of 2007; and
- Publishing the *Overview of the Privacy Act of 1974*, a treatise of Privacy Act case law.

3. COMPONENT RESPONSIBILITIES

The establishment of OPCL as a separate office has more clearly defined the Department's privacy program and the components' responsibilities for compliance with privacy laws, regulations, and policies. During this reporting period, OPCL has continued to work with Department leadership to formally establish the appointment of a Senior Component Official for Privacy (SCOP) at each of the Department's components through a Department directive. Once appointed, the SCOPs will be accountable and responsible for their respective component's privacy program and will coordinate their component's privacy issues and concerns with the CPCLO, OPCL, and Department leadership.

THE PRIVACY COMPLIANCE PROCESS

The Department's collection, maintenance, and use of information about individuals are critical to its ability to effectively enforce the law, defend the interests of the United States, and ensure public safety. As it fulfills these missions, the Department must also fulfill its responsibility to manage and protect the sensitive PII it collects on individuals. Ensuring an appropriate balance between meeting the government's critical information needs while scrupulously guarding against 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.

1. THE INITIAL PRIVACY ASSESSMENT

The privacy compliance process begins when the Department first determines it needs to collect, maintain, disseminate, or otherwise use PII. The Department has established the Initial Privacy Assessment (IPA) template, which consolidates various privacy compliance requirements into a single, unified, and comprehensive process. The IPA template consists of questions designed to

help components and OPCL determine whether a particular information system requires further privacy documentation (e.g., completion of Privacy Impact Assessment or development or modification of a system of records notice (SORN)) or raises other privacy issues or concerns. It also bridges the information technology (IT) security and privacy processes and communities. The Department has incorporated the IPA process into its IT certification and accreditation process and the software application used to track compliance of electronic systems with the FISMA. This certification and accreditation process requires program managers for IT systems, whether 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 PII. Through the IPA process, 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) or other sensitive PII within a system is not necessary. The component can then forgo the collection of such PII in accordance with applicable privacy protection directives and policies. During this reporting period, OPCL reviewed and made determinations on a total of 125 IPAs submitted by Department components.

2. PRIVACY ACT REQUIREMENTS

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.[4] 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 for collection and maintenance, the categories of individuals serving as the subject of such records, the categories of information to be used and collected by the agency, the location where the agency maintains the information, the means of access and correction available to the individual, the security safeguards that will protect the information, and the parties with whom and under what conditions the agency will share the information in the system.[5] The Department of Justice maintains more than 200 systems of records. The SORNs for these systems can be found on OPCL's website at www.justice.gov/opcl/privacyact.html.[6]

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 Privacy Act requirements that govern such information. For example, once OPCL determines that a particular information system qualifies as a system of records, it may be necessary to draft a SORN or modify an existing SORN and any accompanying exemption regulation. OPCL reviews all such SORNs and accompanying exemption regulations for approval and issuance by the CPCLO.[7] Within this SORN review process, OPCL also assists

[4] *See* 5 U.S.C. § 552a (2012).
[5] *See id.* § 552a(e)(4).
[6] There may be several subsystems of records that are covered by the same system of records notice.
[7] The Attorney General delegated his authority to carry out these responsibilities to the CPCLO by order in January 2008.

components in reviewing routine use disclosures included in SORNs to ensure that each routine use disclosure contemplated is compatible with the purpose for which the information was collected.

During this reporting period, OPCL revised the Department's guidance and templates on SORNs and exemption regulations in order to provide better assistance to components when drafting and preparing these documents. The Department also published seven new or modified SORNs and three regulations during this time period. In addition to publishing SORNs and regulations, OPCL advises components on preparing other Privacy Act documents, such as Privacy Act consent forms,[8] and Privacy Act notice statements, which provide actual notice to an individual about an agency's collection authority and the possible uses of information collected from individuals.[9]

3. PRIVACY IMPACT ASSESSMENTS

Section 208 of the E-Government Act of 2002 requires all federal agencies to conduct a Privacy Impact Assessment (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.[10] 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.[11]

By way of the IPA process, OPCL makes final determinations on whether a PIA is required to be completed by the component. In conducting a PIA, the Department considers the privacy impact from the beginning of a system's development through the system's lifecycle 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 IT systems that require PIAs and allows OPCL and Department components to resolve privacy and related security issues before a system is certified and accredited.

During this reporting period, OPCL began updating the Department's PIA template to include more detailed guidelines for properly assessing issues and responding to the questions in the PIA template.[12] The CPCLO reviewed 16 PIAs during this period, and all PIAs for non-national security systems can be found on OPCL's website at www.justice.gov/opcl/pia.htm.

---

[8] *See* 5 U.S.C. § 552a(b).
[9] *See* 5 U.S.C. § 552a(e)(3).
[10] *See* E-Government Act of 2002 § 208, 44 U.S.C. § 3501 (note) (2012).
[11] *See* Office of Management and Budget Memorandum, M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, Attachment A, § II-A(f) (Sept. 26, 2003), *available at* http://www.whitehouse.gov/omb/memoranda_m03-22.
[12] The PIA template, which was modified slightly in March 2012, is available at http://www.justice.gov/opcl/docs/doj-pia-template-march2012.pdf.

LEGAL GUIDANCE AND TRAINING

OPCL attorneys serve as legal counsel for the Department on certain federal information privacy compliance requirements, policies, and initiatives. In this capacity, OPCL advises components about the applicability and requirements of federal information privacy laws, such as the Privacy Act and the E-Government Act, to help components perform their operations and functions while protecting the privacy rights of individuals. In addition, OPCL advises Department components on privacy issues that arise in connection with litigation; develops and conducts privacy training; and reviews pending legislation, Congressional testimony, Executive Orders, and reports.

In 2012, OPCL prepared and issued a revised edition of the *Overview of the Privacy Act of 1974* (*Overview*).[13] This biennial publication provides a thorough and up-to-date legal analysis of the Privacy Act's agency record-keeping requirements, disclosure prohibition, 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. OPCL is currently working on the 2014 edition of the *Overview*.

Finally, 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, topics of OPCL training included: overview of Privacy Act requirements; FISMA reporting; privacy provisions of the E-Government Act of 2002 and PIA drafting; SORN drafting; interface between the privacy provisions of the E-Government Act and the Privacy Act; interface between the Freedom of Information Act and the Privacy Act; litigation concerns involving the Privacy Act; and law enforcement records and the Privacy Act. OPCL staff also conducted component-specific privacy training as well as conducted training at other federal agencies upon request.

PRIVACY POLICY AND LEADERSHIP

1. INTRA-AGENCY LEADERSHIP

Within the Department, the CPCLO and OPCL collaborate and engage with Department components in the development of new policies and programs that affect the Department's handling of PII. Examples of such engagements include:

Open Government Initiatives -- OPCL is an active member of the Department's Web 2.0 Policy Working Group, which formed in 2010 following OMB's issuance of policies governing the implementation of the Administration's Open Government Initiative.[14] The purpose of this working group is to review proposed uses of social media and other new media technologies by the Department for legal and policy issues, such as privacy, ethics, records management, and public affairs. As part of the working group's clearance process, OPCL receives initial privacy

[13] An electronic version of the *Overview* is available at www.justice.gov/opcl/1974privacyact-overview.htm.
[14] *See* Office of Management and Budget Memorandum, M-10-16, *Open Government Directive* (Dec. 8, 2009), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf.

assessments from components seeking to use social media or other new media technologies and reviews them to ensure that the proposed use is consistent with federal privacy laws, such as the Privacy Act of 1974 and Section 208 of the E-Government Act of 2002, and OMB policies, such as those set forth in M-10-23 (Guidance for Agency Use of Third-Party Websites and Applications) and M-03-22 (Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002). OPCL reviewed 26 IPAs for such uses during this reporting period. As new media uses have developed, this working group has also reviewed new Department policies on such uses, including reviewing the Department's use of applications on mobile devices.

Data Breach Response and Reviews -- The CPCLO and OPCL participate in the Department's review of incidents and data breaches in accordance with the Department's Incident Response Procedures.[15] The Incident Response Procedures established a Core Management Team (CMT), which is co-chaired by the CPCLO and the Department's Chief Information Officer. The CPCLO and OPCL are notified of actual or suspected breaches of PII, and provide legal and policy guidance to the CMT regarding the privacy implications associated with data breach incidents and any Department response.

Data Integrity Board -- The CPCLO is also a member of the Department's Data Integrity Board. The Data Integrity Board oversees and coordinates the implementation of the Computer Matching and Privacy Protection Act of 1988, 5 U.S.C.§ 552a(o), 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 two computer matching agreements.

Executive Order 13636 -- In February 2013, the President signed Executive Order 13636, which directs federal departments and agencies to establish, expand, or prioritize a number of activities to improve cybersecurity for U.S. critical infrastructure. Section 5 of the Executive Order requires Senior Agency Officials for Privacy and Civil Liberties to conduct assessments of the privacy and civil liberties risks of their agency activities under the Order based on the Fair Information Practice Principles (FIPPs) and report on such assessments. During this reporting period, the CPCLO and OPCL coordinated with Department leadership to incorporate privacy and civil liberties protections into the Department's implementing instructions, under section 4(a) of the Executive Order, to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The CPCLO and OPCL also worked closely with other Department components to review relevant activities implementing the Order, and to ensure that the FIPPs were and will continue to be appropriately considered and incorporated in such activities.

National Security Reviews -- The CPCLO receives National Security Review (NSR) reports, which include findings and conclusions from audits of different FBI field offices by the National Security Division. The CPCLO reviews these reports to ensure both that FBI field offices are in

[15] The Department's Incident Response Procedures for Data Breaches are available at http://www.justice.gov/opcl/breach-procedures.pdf.

compliance with laws, policies, and procedures designed to protect privacy and civil liberties, and that the NSRs are conducted appropriately.

2. INTER-AGENCY LEADERSHIP

The CPCLO and OPCL also engage in leadership roles within the federal privacy community and increased their participation and role in inter-agency privacy activities during this reporting period. Examples of such participation include:

Information Sharing Environment (ISE) -- The CPCLO and OPCL continue to be active members of the Information Sharing Environment working groups. For example, the CPCLO serves on the Executive Committee of the Privacy and Civil Liberties (PCL) Sub-Interagency Policy Committees (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 (ODNI). 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. OPCL also supports the PCL Sub-IPC on various sub-working groups.

Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) -- The NSI is a partnership for sharing terrorism-related suspicious activity reports (SARs) among federal, state, local, and tribal agencies. 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, state, and local entities while protecting the privacy and other legal rights of Americans.[16] In this reporting period, the CPCLO worked with the Federal Bureau of Investigation, the Program Manager of the ISE (PM-ISE), and other federal privacy officers to review the adoption of a revised Functional Standard for Suspicious Activity Reports in the ISE.[17] In this context, the CPCLO participated in a roundtable of privacy advocates coordinated by the PM-ISE to discuss the proposed revisions and will continue to work in this area as the revisions are further considered.

International Efforts -- 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. The CPCLO also works closely with the Office of International Affairs in the Department's Criminal Division on data protection issues to further enhance international information sharing negotiations. The CPCLO also serves as the U.S. privacy co-lead, along 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. During this reporting period, the CPCLO met with the Canadian delegates to brief delegates on the progress of implementation of the agreed joint privacy principles. As another example of work in the

[16] *See* National Strategy for Information Sharing at 11, *available at* http://ise.gov/sites/default/files/nsis_book_0.pdf.
[17] A*vailable at* http://ise.gov/sites/default/files/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf.

international context, the CPCLO met with members from a German Delegation to discuss international data quality standards, information sharing, and U.S. privacy frameworks.

Federal CIO Council Privacy Committee -- The Privacy Committee serves as the interagency coordination committee for Senior Agency Officials for Privacy and Civil Liberties 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 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 FIPPs.[18] An example of OPCL's participation in the work of the CIO Council is its work on Appendix J of NIST Special Publication 800-53 Revision 4, entitled "Security and Privacy Controls for Federal Information Systems and Organizations," published in April 2013. Appendix J, entitled "Privacy Control Catalogue," provides agencies with an in-depth guide to identifying and implementing privacy controls concerning the use of PII.

Other leadership efforts -- In addition, the CPCLO and OPCL participate in other OMB-led or inter-agency privacy working groups and leadership efforts (e.g., a working group to develop OMB guidance to help federal agencies implement the Do Not Pay (DNP) Initiative under section 5 of the Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA); various working groups created to assess the government's policies on unmanned aerial systems; and meetings with members of the Privacy and Civil Liberties Oversight Board (PCLOB)[19] to discuss Department programs and operations and how privacy and civil liberties issues are considered in the counterterrorism context).

REDRESS

1. PRIVACY AND CIVIL LIBERTIES COMPLAINTS

OPCL receives numerous inquiries from members of the public through its email inbox and main phone number, and has established a process to review such inquiries in a timely manner. In this capacity, OPCL acts as an ombudsman for inquirers to ensure that their inquiries are properly reviewed and responses are properly provided and/or appropriately referred. For this reporting period, OPCL received 616 inquiries from members of the public, of which twelve were considered a privacy and/or civil liberties complaint against the Department.[20] Some examples of the types of privacy and/or civil liberties complaints that were received by OPCL include: a request from an individual seeking assistance to remove information about him from a

[18] For a version of the FIPPs adopted by the White House and cited in Executive Order 13636 (Improving Critical Infrastructure Cybersecurity), see page 45 of the National Strategy for Trusted Identities in Cyberspace, available at http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.
[19] The PCLOB is an independent agency within the Executive branch charged with assisting the President and other senior Executive Branch officials in ensuring that privacy and civil liberties concerns are appropriately considered in the implementation of all laws, regulations, and policies related to efforts to protect the Nation against terrorism.
[20] The other inquiries did not qualify as privacy and/or civil liberties complaints because the matters raised in those inquiries either fell outside the purview of the Office (e.g., the complaints were against private entities or other non-DOJ entities) or did not raise issues concerning privacy and/or civil liberties matters.

Department webpage; a potential unlawful disclosure claim resulting in adverse employment issues; alleged dispute regarding collection of social security numbers on DOJ forms; and allegations regarding insufficient safeguarding of information within a DOJ component. In each of these instances, OPCL worked with the affected component to seek resolution and/or referred the complaints to the appropriate Department offices, such as the Office of the Inspector General, for review.

2. PRIVACY ACT AMENDMENT APPEALS

In addition to receiving general privacy inquiries, OPCL adjudicates all appeals of denials by Department components of requests to amend records under subsection (d)(2) of the Privacy Act. OPCL also adjudicates initial requests to amend records received by the Department's senior management offices. Within the reporting period, OPCL adjudicated 43 Privacy Act amendment appeals.

ACCOUNTABILITY AND REPORTING

The CPCLO and OPCL are responsible for issuing and contributing to numerous Department privacy reports, including: the annual report in accordance with Section 1174 of the Violence Against Women and Department of Justice Reauthorization Act of 2005; the quarterly reports on the activities of the CPCLO and OPCL under Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (803 Reports); the Senior Agency Officials for Privacy and Civil Liberties' sections of the quarterly and annual reports in accordance with the FISMA; annual privacy and civil liberties assessments of the Department's activities under section 5(b) of Executive Order 13636 (Improving Critical Infrastructure Cybersecurity); and the annual report under the Federal Agency Data Mining Reporting Act of 2007. Certain reports from this reporting period that have been approved by OMB and transmitted to Congress can be found on OPCL's webpage at www.justice.gov/opcl/reports.htm. These reports are described in more detail below:

FISMA -- Federal agencies are required to submit annual and quarterly reports to OMB regarding their privacy programs in accordance with the FISMA and OMB guidance implementing the FISMA.[21] The quarterly reports reflect the information provided in the Department's IPAs and help OPCL determine the number of information systems in the Department that collect PII, require a PIA and/or SORN, and for which the Department has completed such documentation. The annual report includes information collected quarterly and also requires the CPCLO and OPCL to collect data and report on the Department's privacy program.

803 Reports -- The CPCLO submits these reports to Congress and the PCLOB on a quarterly basis. The 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 privacy reviews undertaken; the type of advice provided and the response given to such advice; the

[21] *See* 44 U.S.C. § 3544(c) (2012); *see also* http://www.whitehouse.gov/omb/inforeg_infopoltech#pg for annual OMB FISMA guidance.

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.

Data Mining Report -- This report describes the Department's activities that qualify as data mining under the Federal Agency Data Mining Reporting Act of 2007[22] and the privacy and civil liberties protections built into such activities. During this reporting period, OPCL worked with other Department components to streamline the reporting process, and to identify and review privacy and civil liberties procedures in place in such qualifying data mining activities.

Executive Order 13636 -- Executive Order 13636, Improving Critical Infrastructure Cybersecurity (Feb. 19, 2013), aims to strengthen the cybersecurity of critical infrastructure by increasing information sharing and by jointly developing and implementing a framework of cybersecurity practices with the private sector. Section 5(b) of the Executive Order requires Senior Agency Officials for Privacy and Civil Liberties of agencies engaged in activities under the executive order to "conduct assessments of their agency activities," and to provide such assessments to the Department of Homeland Security (DHS) for consideration and inclusion in a yearly DHS report on the privacy and civil liberties risks of functions and programs undertaken by agencies as called for in the Executive Order. Such assessments "shall include evaluation of activities against the Fair Information Practice Principles and other applicable privacy and civil liberties principles, policies, and frameworks."[23] In 2013, OPCL worked closely with Department components and the Assessments Working Group of the DHS Interagency Task Force to draft the Department's initial privacy and civil liberties assessment. As the Department's activities implementing the Executive Order become more fully developed, OPCL will continue to coordinate with Department leadership and Department components to ensure that privacy and civil liberties protections are appropriately incorporated into such activities, as well as to satisfy the yearly reporting requirements of section 5(b) of the Executive Order.

FUTURE INITIATIVES OF THE DOJ PRIVACY PROGRAM

The CPCLO and OPCL are committed to building and sustaining 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 strengthening the Department's components' roles and responsibilities in order to build a successful and accountable privacy program in every component of the Department. The Department will continue to explore innovative and efficient ways to incorporate privacy in the Department's complex and diverse mission work, and looks forward to discussing these new initiatives in the next annual report.

[22] 42 U.S.C. § 2000ee-3 (2012).
[23] Executive Order 13636 (Improving Critical Infrastructure Cybersecurity), § 5(b) (Feb. 19, 2013), *available at*: http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.