U.S. Department of Justice

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

PRIVACY AND CIVIL LIBERTIES ACTIVITIES SEMI-ANNUAL REPORT

FIRST SEMI-ANNUAL REPORT, FY 2015

OCTOBER 1, 2014 – MARCH 31, 2015

United States Department of Justice
Semi-Annual Section 803 Report

Message from the Chief Privacy and Civil Liberties Officer

I am pleased to present the Department of Justice's (Department or DOJ) Semi-Annual Section 803, of the Implementing Recommendations of the 9/11 Commission Act of 2007, 42 U.S.C. § 2000ee-1 (2012), Report. This report covers the period from October 1, 2014, through March 31, 2015.

Specifically, Section 803 requires federal agency semi-annual reports related to the discharge of certain privacy and civil liberties functions of the agency's Senior Agency Official for Privacy (SAOP). The Department's Chief Privacy and Civil Liberties Officer (CPCLO) in the Office of the Deputy Attorney General serves as the SAOP for the Department, and as the Attorney General's principal advisor on privacy and civil liberties matters. The Department's Section 803 reports include the following information:

- The number and types of privacy reviews undertaken by the CPCLO (including reviews of legislation and testimony, initial privacy assessments, privacy impact assessments, system of records notices, Privacy Act exemption regulations, OMB Circular A-130, data breach incidents, Privacy Act amendment appeals), and
- The type and description of advice and outreach undertaken by the CPCLO and the Department's Office of Privacy and Civil Liberties (OPCL).
- The number and nature of privacy complaints received by the CPCLO and OPCL for alleged violations.

Overall, the Department's privacy program is supported by a team of dedicated privacy professionals who strive to reinforce 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.

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
U.S. Department of Justice

I. INTRODUCTION

Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, 42 U.S.C. § 2000ee-1 (2012) (hereinafter "Section 803"), requires designation of a senior official to serve as the Attorney General's principal advisor on privacy and civil liberties matters and imposes reporting requirements of such official on certain activities.[1] The Department of Justice's ("Department" or "DOJ") Chief Privacy and Civil Liberties Officer (CPCLO) in the Office of the Deputy Attorney General serves as the principal advisor to the Attorney General and is supported by the Department's Office of Privacy and Civil Liberties (OPCL). Specifically, Section 803 requires periodic reports[2] related to the discharge of certain privacy and civil liberties functions of the Department's CPCLO, including information on: the number and types of privacy reviews undertaken by the CPCLO; 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 such officer. Many of these functions are discharged, on behalf of the CPCLO, by the Department's OPCL. To provide a standard reportable framework, the Department has coordinated with the Office of Management and Budget (OMB) in order to tailor the report to the missions and functions of the Department's CPCLO.

Accordingly, the Department submits the first Semi-Annual Report for Fiscal Year 2015 on such activities of the Department's CPCLO and OPCL.

II. PRIVACY REVIEWS

The Department conducts privacy reviews of information systems and programs to ensure that privacy issues are identified and analyzed in accordance with federal privacy laws enumerated in controlling authorities such as the Privacy Act of 1974, 5 U.S.C. § 552a (2012), the privacy provisions of the E-Government Act of 2002, 44 U.S.C. § 3501 (note) (2012), as well as federal privacy policies articulated in Office of Management and Budget (OMB) guidance, including OMB Circular A-130.[3]

A privacy review for purposes of this report encompasses activities that are part of a systematic and repeatable process such as those listed below:

---

[1] *See* 42 U.S.C. § 2000ee-1 (2014).

[2] On July 7, 2014, the statute was amended to require semiannual submissions of the periodic reports rather than quarterly submissions. *See id*. § 2000ee-1(f) (2014), Pub. L. No. 113-126, Title III, § 329(b)(4), 128 Stat. 1406 (2014).

[3] *See* OMB Circular No. A-130, Management of Federal Information Resources, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals, 61 Fed. Reg. 6428 (Feb. 20, 1996), *as amended*, 65 Fed. Reg. 77,677 (Dec. 12, 2000), *available at*: http://www.whitehouse.gov/omb/circulars_a130.

1. **Proposed legislation, as well as testimony, and reports prepared by departments and agencies within the Executive Branch:**
   Proposed legislation, testimony, and reports are reviewed for any privacy and civil liberties issues by OPCL and the CPCLO.

2. **Initial Privacy Assessment (IPA)**:
   An IPA is a privacy compliance tool developed by the Department of Justice as a first step to: facilitate the identification of potential privacy issues; assess whether privacy documentation is required; and ultimately ensure the Department's compliance with applicable privacy laws and policies.[4] IPAs are conducted by Department components with coordination and review by OPCL. For purposes of this report, this number represents IPAs that have been reviewed and closed by OPCL.

3. **Privacy Impact Assessment (PIA):**
   A PIA is an analysis, required by Section 208 of the E-Government Act of 2002, of how information in identifiable form is processed to: ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[5] For purposes of this report, this number represents PIAs that have been reviewed, approved and/or closed by OPCL and/or the CPCLO.

4. **System of Records Notice (SORN):**
   A SORN is a notice document required by the Privacy Act of 1974 which describes the existence and character of a system of records, including the categories of individuals whose records are in the system; the categories of records; and the routine uses of the records.[6] The SORN is published in the Federal Register. For purposes of this report, this number represents SORNs reviewed and approved by OPCL and the CPCLO that result in a published SORN for which the comment period has exhausted.

[4] For further information about the Department's IPA process, *see* http://www.justice.gov/opcl/privacy-compliance-process.

[5] *See* OMB Memorandum, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Attachment A, Section II.A.6 (Sept. 26, 2003), *available at*: http://www.whitehouse.gov/omb/memoranda_m03-22.

[6] *See* 5 U.S.C. § 552a(e)(4).

5. **Privacy Act Exemption Regulation:**
The Privacy Act provides that agencies may exempt some systems of records from certain provisions of the Act. A Privacy Act exemption regulation is the regulation promulgated by an agency and published in the Federal Register that provides the reasons why a system of records maintained by the agency is exempt from certain provisions of the Act.[7] For purposes of this report, this number represents exemption regulations that have been reviewed and approved by OPCL and the CPCLO that results in a final regulation for which the comment period has exhausted.

6. **Information Collection Notice:**
An information collection notice is a notice to individuals as required by subsection (e)(3) of the Privacy Act.[8] The notice, which must be on the form used to collect the information or on a separate form that the individual can retain, includes the authority for collecting the information; the principal purpose for which the information is intended to be used; the routine uses of the information; and the effects on the individual, if any, of not providing all or any of part of the requested information. For purposes of this report, this number represents reviews of information collection notices conducted by OPCL to ensure that they fully meet the requirements of subsection (e)(3) of the Privacy Act.

7. **OMB Circular A-130:**
OMB Circular A-130 reviews include assessments of the following: SORNs to ensure that they are accurate and up to date; routine uses to ensure that they are still required and compatible with the purpose for which the information was collected; record practices and retention schedules to ensure that they are still appropriate; exemption regulations to ensure that they are still necessary; contracts to ensure that appropriate Federal Acquisition Regulation language is used to bind the contractor to provisions of the Privacy Act; Computer Matching programs to ensure compliance; civil or criminal violations of the Privacy Act to assess concerns; and agency programs for any privacy vulnerabilities.[9] For purposes of this report, this number represents the systems of records that have been reviewed in accordance with the requirements of OMB Circular A-130 by Department components and submitted to OPCL. These reviews are conducted on an annual basis in coordination with the Federal Information Security Management Act (FISMA)[10] reviews. Specific details of such FISMA reviews are submitted through the annual FISMA report.

---

[7] *See id.* § 552a(j), (k).
[8] *See id.* § 552a(e)(3).
[9] *See* OMB Circular No. A-130, Management of Federal Information Resources, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals, 61 Fed. Reg. 6428 (Feb. 20, 1996), *as amended*, 65 Fed. Reg. 77,677 (Dec. 12, 2000), *available at:* http://www.whitehouse.gov/omb/circulars_a130.
[10] 44 U.S.C. § 3541 *et seq*. (2014).

8. **Data Breach or Incident:**
   A data breach or incident includes intentional or inadvertent losses of personally identifiable information (PII) in the control of the Department or its contractors who process, store, or possess DOJ PII.[11] For purposes of this report, this number includes data breaches and incidents that have been formally reviewed by the Department's Core Management Team (DOJ's organizational team chaired by the CPCLO and the Chief Information Officer, which convenes in the event of a significant data breach involving PII).

9. **Privacy Act Amendment Appeal:**
   A Privacy Act amendment appeal is an appeal of an initial agency action regarding a request from an individual to amend their information that is maintained in a Privacy Act system of records.[12] For purposes of this report, this number represents the number of appeals that have been adjudicated and closed by OPCL.

PRIVACY REVIEWS	
Type of Review	**Number of Reviews**
Legislation, testimony, and reports	111
Initial Privacy Assessments	10
Privacy Impact Assessments	5[13]
Data breach and incident reviews	1

[11] The Department's Instruction titled "Incident Response Procedures for Data Breach" is *available at* http://www.justice.gov/opcl/breach-procedures.pdf.

[12] *See* 5 U.S.C. § 552a(d)(2), (3).

[13] During this reporting period, the Department of Justice (DOJ) completed five PIAs. One PIA pertains to a national security system. Although not required by the E-Government Act of 2002, pursuant to section 202(i), 44 U.S.C. § 3501 note, the Department conducts PIAs for a Departmental national security system if a system collects information in identifiable form on individuals as a matter of policy. National security PIAs are not subject to the PIA publication requirement.

PRIVACY REVIEWS	
Type of Review	**Number of Reviews**
(e)(3) Notices – • The Office of Community Oriented Policing Services (COPS) – Presidential Task Force on 21st Century Policing • The Bureau of Prisons (BOP) – CJIS Name Check Request, Non-U.S. Citizen Name Check	2

III. PRIVACY IMPACT ASSESSMENTS

The Department is committed to ensuring the appropriate protection of privacy and civil liberties in the course of fulfilling its missions. PIAs, which are required by Section 208 of the E-Government Act of 2002, are an important tool to assist the Department in achieving this objective. Below are executive summaries of DOJ's PIAs published for public review for this period, along with a hyperlink to the full text.

- **FBI Next Generation Identification (NGI) Retention and Searching of Noncriminal Justice Fingerprint Submissions**

FBI's Next Generation Identification (NGI) is a system designed to replace the FBI's Integrated Automated Fingerprint Identification System (IAFIS). NGI will provide new and advanced services for other biometrics. This PIA addresses the retention and searching of civil (noncriminal justice) fingerprints submitted by federal agencies as well as the retention and searching of civil fingerprints submitted by state, local, and tribal agencies. The FBI developed NGI to retain civil fingerprints when authorized by the submitting agency, and to consolidate those civil fingerprint submissions, along with accompanying biographic data into a single identity record. The retention and searching of these civil fingerprints is authorized only for those individuals whose employment, license, or other benefit requires that the individual not commit a prohibited criminal action. This PIA has been published on FBI's website and is located at: http://www.fbi.gov/foia/privacy-impact-assessments/next-generation-identification-ngi-retention-and-searching-of-noncriminal-justice-fingerprint-submissions.

- **FBI Next Generation Identification (NGI) Palm Print and Latent Fingerprint Files**

This PIA describes some of the enhancements made to NGI, including the development of a National Palm Print System (NPPS) and enhanced searching of latent fingerprints. To make them searchable and retrievable, previously collected hard copy palm prints have been converted

to electronic format. This PIA is located at: http://www.fbi.gov/foia/privacy-impact-assessments/next-generation-identification-palm-print-and-latent-fingerprint-files.

- **DOJ Giglio Information Systems**

The purpose of the Department's Giglio information file systems is to enable prosecuting offices to disclose potential impeachment information to defense counsel in federal criminal prosecutions. This PIA reflects updates to the Department's Giglio policy and covers multiple individual Giglio information systems. This PIA also provides notice of the Department's maintenance of such information to Government employees as well as to defense counsel and members of the public. The purpose of each Giglio information system is to permit prosecuting offices to maintain a more organized, logical, and comprehensive filing system, searchable by the witness's or affiant's name. This PIA has been published on OPCL's website and is located at: http://www.justice.gov/opcl/doj-privacy-impact-assessments.

- **Justice Management Division (JMD) Justice Unified Telecommunications Network (JUTNet) Voice Services System**

The Justice Unified Telecommunications Network (JUTNet) is the Department's wide area network. This PIA covers the JUTNet Voice Services system (JVS), a telephone and voicemail system that operates on JUTNet. JVS is designed to replace legacy telephone and voicemail systems and comprises two subsystems: the Cisco Unity Voicemail system (CUV) and the DOJ enterprise Voice Over Internet Protocol system (VOIP). This PIA is located at: http://www.justice.gov/sites/default/files/opcl/pages/attachments/2015/01/06/jvs_pia_final_1-6-2015_pdf.pdf.

IV. ADVICE AND OUTREACH

Formal advice encompasses the issuance of formal written policies, procedures, guidance, or interpretations of privacy requirements for circumstances or business processes. This advice has been drafted or authorized by the CPCLO and approved as official agency policy by Department leadership to respond to issues or concerns regarding safeguards for privacy and civil liberties. Examples of formal advice and responses to advice provided may include issuance of regulations, orders, guidance, agreements, or training. For this semi-annual period, the CPCLO or OPCL did not provide any formal written guidance.

On November 17, 2014, the CPCLO and OPCL hosted an event on various emerging privacy issues for Department employees. The Privacy Forum, an inaugural event, consisted of panels, such as Big Data and Emerging Technologies, and was attended by the Deputy Attorney General who provided opening remarks to the attendees.

The CPCLO and OPCL have continued to engage stakeholders in the privacy community. They have conducted outreach to the privacy advocacy community and participated in a number of speaking engagements to promote transparency of the Department's policies, initiatives, and oversight with respect to the protection of privacy and civil liberties. The following activities highlight some of the CPCLO and OPCL's efforts:

- The CPCLO and OPCL continued to meet with the European Delegation regarding E.U.-U.S. Data Protection and Privacy Agreement (DPPA) negotiations. In concert with such negotiations, the CPCLO and OPCL led a process that included federal agencies to develop proposed legislation that extends to citizens of certain countries the core benefits that Americans enjoy under the Privacy Act with regard to information shared with the United States for law enforcement purposes. This proposed bill, H.R. 1428, introduced on March 18, 2015, and titled "Judicial Redress Act of 2015", has been referred to committee for further consideration.
- The CPCLO and OPCL met with the Privacy and Civil Liberties Oversight Board (PCLOB) to discuss the Department's privacy training programs.
- On October 9 and 10, 2014, the CPCLO participated in an American Bar Association (ABA) event, titled "Antitrust Masters Course VII," hosted by the ABA Section on Antitrust Law. On October 9, 2014, the CPCLO was a keynote speaker at the luncheon. On October 10, 2014, the CPCLO participated on a panel titled "Hot Antitrust and Consumer Protection Issues for High-Tech Companies." This panel focused on "hot topics" in antitrust and consumer protection relating to high technology that are the subject of recent agency enforcement actions and private litigation.
- On October 30, 2014, the CPCLO participated in roundtables at the "Big Data and Civil Rights Conference" hosted by the Data & Society Research Institute, the Leadership Conference on Civil and Human Rights, and New America's Open Technology Institute.
- On November 12, 2014, the CPCLO presented on a panel entitled "What privacy interests have government privacy officials identified and how are they addressed in the counterterrorism context?" as part of the Defining Privacy Conference hosted by the Privacy and Civil Liberties Oversight Board.
- On December 2, 2014, the Director of OPCL participated on a panel titled "The Privacy Act at 40" as part of an International Association of Privacy Professionals (IAPP) Practical Privacy Series. This panel discussed whether the Privacy Act of 1974 is sufficient for the challenges of today's technology and society.
- On February 12, 2015, the CPCLO participated on a panel titled "The Internet of Things: Big Data and You" hosted by George Washington University's Trachtenberg School of Public Policy and the ABA's Consumer Protection Section. This panel discussed the potential benefits and challenges, including data security and transparency and choice, of utilizing connected electronic devices.

- On February 20, 2015, the CPCLO and OPCL met with members of the civil society advocacy community to discuss making privacy compliance information more accessible and how to use Big Data to support greater openness and accountability. These meetings were hosted by the White House's Office of Science and Technology Policy (OSTP).
- On March 5, 2015, the CPCLO participated on a panel titled "The Job of Protecting Both the Nation's Security and Privacy" as part of IAPP's 2015 Summit. This panel included Chief Privacy Officers from various federal agencies to discuss their roles and the role of a privacy office within organizations that have national and homeland security missions.

V. COMPLAINTS

A privacy complaint encompasses a written allegation (excluding complaints filed in litigation against the Department) concerning a violation of privacy protections in the administration of the programs and operations of the Department that is submitted to or through the CPCLO and/or OPCL. Complaints directly received by components without notice to the CPCLO and/or OPCL are handled by components and are not counted for purposes of this report. Privacy complaints are separated into three categories:

1. Process and procedural issues (such as appropriate consent, collection and/or notice);
2. Redress issues (such as misidentification or correction of personally identifiable information, which are outside of the Privacy Act amendment process); and
3. Operational issues (inquiries regarding general privacy, including Privacy Act matters).

A civil liberties complaint encompasses a written allegation (excluding complaints filed in litigation against the Department) for a problem with or violation of civil liberties safeguards concerning the handling of personal information by the Department in the administration of Department programs and operations that is submitted to or through the CPCLO and/or OPCL.

For each type of privacy or civil liberties complaint received by the CPCLO and/or OPCL during the quarter, the report will include the number of complaints in which (1) responsive action was taken or (2) no action was required. In the event a complaint is received within five business days of the last day of the close of the quarter, the complaint may be counted and addressed in the subsequent quarter if time constraints hinder a thorough examination of the complaint in the quarter in which received.

PRIVACY AND/OR CIVIL LIBERTIES COMPLAINTS[14]				
Type of Complaint	**Number of Complaints**	**Disposition of Complaint**		
		Referred to Component for review	**Referred to Office of Inspector General**	**Referred to another Component or Agency for review**
Process and Procedure	2	2	0	0
Redress	0	0	0	0
Operational	0	0	0	0
Civil Liberties Complaints	0	0	0	0
Total	**2**			

[14] For the First Semi-Annual Report for Fiscal Year 2015, OPCL received 187 inquiries in the form of phone calls, emails, or letters from members of the public, non-federal entities, and within the Department. After a thorough review, OPCL determined that two of the inquiries received qualified as a privacy and/or civil liberty complaint against the Department. One complaint involved a question regarding a litigation filing. The second complaint involved a referral to a state agency. 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.