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 2018

OCTOBER 1, 2017 – MARCH 31, 2018

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 Semi-Annual Report for the period from October 1, 2017 through March 31, 2018 as required by Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, 42 U.S.C. § 2000ee-1 (2012). Section 803 directs the Senior Official for Privacy, who at the Department of Justice is the Chief Privacy and Civil Liberties Officer (CPCLO), to provide 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).
- The type and description of advice 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 and a summary of the disposition of such complaints.
- The outreach to the public informing it about the activities of the CPCLO.
- The other functions of the CPCLO and OPCL.

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 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.

Peter A. Winn
Acting 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 on certain activities of such official.[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 on these matters 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 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. To provide a standard reportable framework, the Department has coordinated with the Office of Management and Budget (OMB) in order to tailor this report to the missions and functions of the Department's CPCLO.

II. PRIVACY REVIEWS

Pursuant to Section 803, "information on the number and types of reviews undertaken" are included in this First Semi-Annual Report for Fiscal Year 2018.[3] Among these are the reviews the Department conducts of information systems and other programs to ensure that privacy issues are identified and analyzed in accordance with federal privacy laws such as the Privacy Act of 1974, 5 U.S.C. § 552a (2012), the privacy provisions of Section 208 of the E-Government Act of 2002, 44 U.S.C. § 3501 (note) (2012), as well as federal privacy policies articulated in OMB guidance, including OMB Circular A-130.[4] Regular reviews conducted pursuant to the requirements of Section 803 include the following:

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 Assessments (IPA):**
   An IPA is a privacy compliance tool developed by the Department 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

[1] *See* 42 U.S.C. § 2000ee-1 (2012).
[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) (201), Pub. L. No. 113-126, Title III, § 329(b)(4), 128 Stat. 1406 (2014).
[3] *See* 42 U.S.C. § 2000ee-1(f)(2)(A).
[4] *See* OMB Circular No. A-130, Managing Information as a Strategic Resource, 81 Fed. Reg. 49689 (July 28, 2016), https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

applicable privacy laws and policies.[5] 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 Assessments (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.[6] 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 Notices (SORN):**
A SORN is a notice document required by the Privacy Act of 1974 that 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.[7] 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.

5. **Privacy Act Exemption Regulations:**
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.[8] For purposes of this report, this number represents exemption regulations that have been reviewed and approved by OPCL and the CPCLO that result in a final regulation for which the comment period has exhausted.

6. **Information Collection Notices:**
An information collection notice is a notice to individuals as required by subsection (e)(3) of the Privacy Act.[9] 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 purposes 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.

---

[5] For further information about the Department's IPA process, *see* http://www.justice.gov/opcl/privacy-compliance-process.
[6] *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), https://obamawhitehouse.archives.gov/omb/memoranda_m03-22/.
[7] *See* 5 U.S.C. § 552a(e)(4).
[8] *See id.* § 552a(j), (k).
[9] *See id.* § 552a(e)(3).

7. **Assessments required by 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.[10]

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 Modernization Act (FISMA)[11] reviews. Specific details of such FISMA reviews are submitted through the annual FISMA report.

On July 28, 2016, OMB released an update to OMB Circular A-130 titled, *Managing Information as a Strategic Resource*.[12] OMB Circular A-130 serves as the governing document for the management of federal information resources. Appendix II to OMB Circular A-130, *Responsibilities for Managing Personally Identifiable Information*, outlines many of the responsibilities for agencies managing information resources that involve personally identifiable information (PII). These responsibilities include a number of requirements for agencies to integrate their privacy programs into their Risk Management Framework, including but not limited to, the selection, implementation, and assessment of the Appendix J[13] privacy controls. OPCL is currently collaborating with the Department's Office of the Chief Information Officer (OCIO) to ensure that all requirements outlined in OMB Circular A-130 are satisfied.

8. **Data Breaches or Incidents:**
The DOJ Instruction 0900.00.01, *Reporting and Response Procedures for a Breach of Personally Identifiable Information,* was updated during the reporting period to account for OMB Memorandum M-17-12 requirements. The Instruction defines a data breach as "the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information (PII) or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose. It includes both intrusions (from outside the organization) and misuse (from within the organization)." In addition, the Instruction defines an incident as "An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or

[10] *See* OMB Circular No. A-130, Managing Information as a Strategic Resource, 81 Fed. Reg. 49689 (July 28, 2016), https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.
[11] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014).
[12] *See* OMB Circular No. A-130, Managing Information as a Strategic Resource, 81 Fed. Reg. 49689 (July 28, 2016), https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.
[13] NIST Special Pub. 800-53 rev. 4 (Apr. 2013).

availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies." The Instruction applies to all DOJ components and contractors who operate systems supporting DOJ. For this reporting period, the Instruction is not yet publically available in full. 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 Appeals:**
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.[14] 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	176
Initial Privacy Assessments	10
Privacy Impact Assessments • Eventbrite[15] • JMD Justice Enterprise File Sharing (JEFS) System[16] • FBI Justice Connect[17]	3
System of Records Notices[18] • JUSTICE/DOJ-018, "DOJ Threat Program Records" • JUSTICE/OIG-006, "OIG Data Analytics Program Records" • JUSTICE/FBI-004, "FBI Online Collaboration System" • JUSTICE/OJP-015, "OJP National Missing and Unidentified Persons System"	4
Notices of Proposed Rule Making • JUSTICE/OIG-006, "OIG Data Analytics Program Records" • JUSTICE/FBI-004, "FBI Online Collaboration System"	2
Data breach and/or incident reviews	0
Privacy Act Amendment Appeals	2

[14] *See* 5 U.S.C. § 552a(d)(2), (3).
[15] DOJ Eventbrite PIA, https://www.justice.gov/doj_eventbrite/download.
[16] DOJ JEFS PIA, https://www.justice.gov/jefs_pia/download.
[17] FI Justice Connect PIA, https://www.fbi.gov/file-repository/pia-justiceconnect.pdf/view.
[18] DOJ SORNs, https://www.justice.gov/opcl/doj-systems-records.

III. ADVICE

Pursuant to Section 803, "the type of advice provided and the response given to such advice" is included in the First Semi-Annual Report for Fiscal Year 2018.[19] The CPCLO's responsibilities include the provision of both formal and informal advice addressing the issuance of formal written policies, procedures, guidance, or interpretations of privacy requirements for certain circumstances or business processes. This advice has been drafted or authorized by the CPCLO to respond to issues or concerns regarding safeguards for privacy and civil liberties and relates to the issuance of regulations, orders, guidance, agreements, or training. The CPCLO received appropriate responses to the formal and informal advice provided.

For this semi-annual period, the CPCLO and OPCL continued working with DOJ components and inter-agency partners to address international privacy questions affecting the Department, as well as international privacy matters, which included discussions with the United Nations Special Rapporteur on Privacy.

The CPCLO and OPCL attended the International Conference of Data Privacy and Protection Commissioners, which is an organization comprising 110 privacy and data protection authorities from across the world that provides leadership at the international level in data protection and privacy. In October 2017, the CPCLO and OPCL attended the 39th International Conference of Data Privacy and Protection Commissioners (ICDPPC). The CPCLO and OPCL Deputy Director attended both the closed sessions for Data Protection Authorities and the open session for invited representatives from industry, academia, and other non-governmental entities.

The CPCLO and OPCL co-developed *The Department of Justice (DOJ) Security and Privacy Assessment and Authorization Handbook* that outlines the process, documentation requirements, and automated tools essential to performing the successful security and privacy assessment and authorization of all DOJ information systems. Based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems, and the Committee on National Security Systems Policy (CNSSP) No. 22, Information Assurance Risk Management Policy for National Security Systems, the DOJ security and privacy assessment and authorization process has been designed to align with existing policy, standards, and guidance, resulting in the assurance that security and privacy controls for DOJ information systems are selected, implemented, and assessed in accordance with established DOJ requirements.

IV. COMPLAINTS

Pursuant to Section 803, "the number and nature of the complaints received by the department, agency, or element concerned for alleged violations" are included in the First Semi-Annual Report for Fiscal Year 2018.[20] 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

[19] *See* 42 U.S.C. § 2000ee-1(f)(2)(B).
[20] *See* U.S.C. § 2000ee-1(f)(2)(C).

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 that are outside of the Privacy Act amendment process (such as misidentification or correction of personally identifiable information); 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 reporting period, 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 a semi-annual period, the complaint may be counted and addressed in the subsequent semi-annual period if time constraints hinder an examination of the complaint in semi-annual period in which it is received.

In addition to privacy and civil liberties complaints concerning the Department, OPCL receives privacy and civil liberties concerns, as defined above, that may pertain to another Federal agency. OPCL responds to these concerns with information on how to contact the appropriate agency to handle their concern. The number of inquiries and the disposition are reflected in the table below.

PRIVACY AND/OR CIVIL LIBERTIES COMPLAINTS[21]				
Type of Complaint	**Number of Complaints**	**Disposition of Complaint**		**Inquiries for Outside the Department**
		Referred to Component for review	**Referred to Office of Inspector General**	**Referred to another Agency for review**
Process and Procedure	0	0	0	10
Redress	0	0	0	1
Operational	0	0	0	11
Civil Liberties Complaints	0	0	0	0

[21] For the First Semi-Annual Report for Fiscal Year 2018, OPCL received 299 inquiries in the form of phone calls, emails, or letters from members of the public, non-federal entities, and within the Department. After a review, OPCL determined that zero of the inquiries received qualified as a privacy and/or civil liberty complaint against the Department. The 299 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.

PRIVACY AND/OR CIVIL LIBERTIES COMPLAINTS[21]				
Type of Complaint	**Number of Complaints**	**Disposition of Complaint**		**Inquiries for Outside the Department**
		Referred to Component for review	**Referred to Office of Inspector General**	**Referred to another Agency for review**
Total	0			22

V. INFORMING THE PUBLIC

Pursuant to Section 803, the CPCLO shall "otherwise inform the public of the activities of such officer, as appropriate and in a manner consistent with the protection of classified information and applicable law."[22] The CPCLO and OPCL have continued to engage stakeholders in the privacy community. They have conducted outreach to the privacy advocacy community, the technology industry, and international organizations. The CPCLO also 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.

VI. OTHER FUNCTIONS

Pursuant to Section 803, the First Semi-Annual Report for Fiscal Year 2018 "shall include information on the discharge of each of the functions of the officer concerned," which include the following additional functions of the CPCLO.[23] Throughout the reporting period, the CPCLO and OPCL have also worked with the Privacy and Civil Liberties Oversight Board and OMB to address privacy concerns, as well as ways to improve agency outreach. Moreover, the CPCLO and OPCL have met with other Federal agencies to improve inter-agency coordination, and to discuss agency privacy practices and common concerns. These meetings enable OPCL to review and assess the Department's information and privacy-related policies, and make improvements where appropriate and necessary.

The CPCLO and OPCL have also worked on several projects for the Federal Privacy Council, including teaching an introductory privacy law class to a wide group of agency privacy officials at a Privacy "Bootcamp" and contributing to the Federal Privacy Council's Executive Committee.

[22] *See* 42 U.S.C. § 2000ee-1(g)(2).
[23] *See* 42 U.S.C. § 2000ee-1(f)(2).