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 QUARTERLY REPORT

SECOND QUARTER, FY 2014

JANUARY 1, 2014 – MARCH 31, 2014

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 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 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.[2] 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, in accordance with Section 803, the Department submits the Second Quarter Report for Fiscal Year 2014 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] *See id*. §2000ee-1(f) (2014), Pub. L. No. 113-126, Title III, § 329(b)(4), 128 Stat. 1406 (2014). On July 7, 2014, the statute was amended to require semiannual submissions of the periodic reports rather than quarterly submissions. Because the Second Quarter of FY 2014 covers activities prior to the amendment of the statute, the Department submits this report on a quarterly basis.

[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. Reviews of proposed legislation, testimony, and reports for privacy and civil liberties issues.
2. Initial Privacy Assessment (IPA) reviews – 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) reviews – 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) reviews – A SORN is a notice document required by the Privacy Act of 1974, which describes the existence and character of a system of records.[6] 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 regulation reviews – A Privacy Act exemption regulation is a regulation promulgated by an agency that maintains a system of records which exempts such system 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 notices reviews – An information collection notice is a notice as required by subsection (e)(3) of the Privacy Act.[8] 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.

---

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

[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).

[7] *See id.* § 552a(j), (k).

[8] *See id.* § 552a(e)(3).

7. OMB Circular A-130 privacy reviews – 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 and specific details of such FISMA reviews are submitted through the annual FISMA report.
8. Data breach and incident reviews – 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. 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 which convenes in the event of a significant data breach involving PII).[11]
9. Privacy Act amendment appeal reviews – 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.

---

[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).

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

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

PRIVACY REVIEWS	
Type of Review	**Number of Reviews**
Legislation, testimony, and reports	84
Initial Privacy Assessments	3
Privacy Impact Assessments	2
Data breach and incident reviews	1
Privacy Act amendment appeals	6

III. PRIVACY IMPACT ASSESSMENTS

During the reporting period, the Department of Justice completed and published PIAs for the Federal Bureau of Investigation (FBI) and the Bureau of Prisons (BOP). The Department of Justice 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 is an executive summary of each of these PIAs, along with a hyperlink to the full text.

- **FBI eGuardian PIA Update**

The Guardian Program, managed by the FBI's Counterterrorism Division (CTD), Guardian Management Unit (GMU), provides a proven methodology for collecting, vetting, reporting, sharing, analyzing, tracking, and mitigating a large volume of Counterterrorism based incidents. The eGuardian system's primary purpose is to facilitate the reporting, tracking, and management of threats to determine whether a particular matter should be closed or opened as a predicated investigation. This PIA update amends the previous eGuardian PIA, dated January 4, 2013, and specifically examines updates to eGuardian as it accounts for privacy concerns while creating an environment which will continue to address the need to share suspicious activity reports (SARs) and threat information as mandated by National Security Presidential Directives. This update is intended to reflect language and policy changes regarding the eGuardian system as it pertains to: record retention of information in eGuardian originating from federal, state, local, tribal and territorial and law enforcement partners, which include fusion centers; and eGuardian becoming the primary Shared Data Repository (SDR) for SARs by such centers. The eGuardian PIA update is available at: http://www.fbi.gov/foia/privacy-impact-assessments/eguardian-threat.

- **BOP Trust Fund Accounting System (TRUFACS)**

TRUFACS is a real-time information system for processing inmate financial information pursuant to commissary-related transactions. Data collected and stored in the system captures financial transactions (e.g., commissary deposits and withdrawals; purchase and resale of approved commissary products; the payment of court-ordered fines and restitution; medical co-payments, and telephone transactions). Information contained in TRUFACS is also necessary for investigative purposes to track suspicious communications, events and transactions, in order to detect potential patterns of criminal activity or fraud (e.g., deposits from unauthorized sources). In general, collection of this information by BOP staff is necessary to meet its federal law obligations to provide managerial oversight and maintain record-keeping responsibility for all financial transactions conducted by current and former inmates. The TRUFACS PIA is available at: http://www.bop.gov/foia/trufacs.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.

During this quarter, formal advice included the following:

- The Deputy Attorney General issued a Department Order which set forth roles and responsibilities of the Department's CPCLO, Heads of Components, and Senior Components Officials for Privacy (SCOPs) regarding privacy and civil liberties matters.
- OPCL provided its annual training to Department of Justice employees and other federal agencies on the Privacy Act of 1974, the E-Government Act of 2002, and the Department's privacy compliance process and reporting requirements.

In addition, the CPLCO and OPCL have provided outreach to the privacy advocacy community and participated in number of speaking engagements in order to promote transparency of the Department’s privacy compliance program. The following events highlight some of the CPCLO/OPCL’s outreach efforts:

- RSA Conference: The CPCLO served as a guest speaker on a panel titled: “Watching the Watchers: The New Privacy Officers Inside the U.S. Government.”

- Meeting with Privacy Advocates: The CPCLO and OPCL representatives met with privacy advocates during this reporting period to discuss the Department's privacy initiatives and provided an overview of the Department's privacy compliance program.
- The Social, Cultural & Ethical Dimensions of "Big Data" Conference: The CPCLO participated in a conference co-hosted by the White House Office of Science and Technology Policy, the Data & Society Research institute, and the New York University Information Law Institute. The conference was part of the 90-day study of big data and privacy led by John Podesta, Counselor to the President, to review, as President Obama stated on January 17, 2014, "how the challenges inherent in big data are being confronted by both the public and private sectors; whether we can forge international norms on how to manage this data; and how we can continue to promote the free flow of information in ways that are consistent with both privacy and security."
- ABA Spring Meeting: The CPCLO moderated a panel titled: "Reclaim Your Name: Privacy in the Era of Big Data." The panel addressed the latest federal and legislative developments, as well as trends regarding big data, and the implications for business practices.

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. 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.

PRIVACY AND/OR CIVIL LIBERTIES COMPLAINTS[13]				
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	0	0	0	0
Redress	0	0	0	0
Operational	0	0	0	0
Civil Liberties Complaints	0	0	0	0
Total	**0**			

[13] For the Second Quarter of FY 2014, OPCL received 65 inquiries in the form of phone calls, emails, or letters from members of the public, non-federal entities, and from within the Department. After a thorough review, OPCL determined that none of the inquiries received qualified as a privacy and/or civil liberties complaint against the Department. The 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.