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

THIRD QUARTER, FY 2014

APRIL 1, 2014 – JUNE 30, 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 ("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, in accordance with Section 803, the Department submits the Third 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] 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). Because the Third 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.[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 which convenes in the event of a significant data breach involving PII).
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 at*: 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	59
Initial Privacy Assessments	5
Privacy Impact Assessments	4
System of Records Notices reviews	1
Information collection notices reviews	3
Privacy Act amendment appeals	1

A. PRIVACY IMPACT ASSESSMENTS

During the reporting period, the Department of Justice completed and published PIAs for the Office on Violence Against Women (OVW), the Federal Bureau of Investigation (FBI), and the Drug Enforcement Administration (DEA). 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.

- **OVW's Peer Reviewer Database**

The Peer Reviewer Database (Database) is a system that allows the Office on Violence Against Women (OVW) to select individuals to serve as grant application reviewers during the peer review process in connection with OVW's annual administration of grant awards. Every year, OVW posts solicitations for its numerous grant programs authorized by the Violence Against Women Act. Federal funding through grants and cooperative agreements enable communities to increase their capacity to respond to crimes of domestic violence, dating violence, sexual assault, and stalking. Each year OVW receives far more applications for grant funding than it can possibly fund. OVW assembles peer review panels comprised of experts and practitioners to help evaluate and score grant applications based on the requirements outlined in the different solicitations for the OVW grant programs. The Database maintains a reviewer's name and contact information. Reviewers may also upload a resume or curriculum vitae (CV) as well as self-identified information such as employee type, job categories, and expertise areas. On a voluntary basis, reviewers may provide their gender, education level and ethnicity. The Peer Reviewer Database PIA is available at: http://www.justice.gov/sites/default/files/opcl/docs/ovw-pia-peer-review-database.pdf.

- **FBI's National Data Exchange (N-DEx)**

N-DEx is a major component of the Department of Justice (DOJ) Law Enforcement Information Sharing Program (LEISP) strategy, a principal purpose of which is to ensure that DOJ criminal law enforcement information is available to users at all levels of government so that they can more effectively investigate, disrupt, and deter criminal activity, including terrorism, and protect national security. The N-DEx PIA was rewritten to reflect technical updates to the system. N-DEx provides a national investigative information sharing system available through a secure Internet site that allows criminal justice agencies to search and analyze data representing the entire criminal justice cycle, including crime incident and investigation records; arrest, booking, and incarceration records; and probation and parole records. As a repository of information from local, state, regional, tribal, and federal criminal justice entities, N-DEx provides these agencies with the capability to make linkages between crime incidents, criminal investigations, and related events to help solve, deter, and prevent crimes. N-DEx contains the personally identifiable information (PII) of suspects, perpetrators, witnesses and victims, and anyone else who may be identified in a law enforcement report concerning a crime incident or criminal investigation. The NDex PIA is available at: http://www.fbi.gov/foia/privacy-impact-assessments/N-DEx.

- **FBI's SENTINEL**

SENTINEL provides management for cases, records, tasks, workflow, and collected items, as well as search and reporting capabilities that will replace the current, paper-based case management system and its associated functions. The primary mission of SENTINEL is to provide the FBI with a browser-based solution for case management. Through the SENTINEL system, employees are able to perform all of the operations related to the creation and management of case-related work items, including action items, leads, collected item records, and the forms used for documenting investigations. Also, discovery of information contained in cases, both open and closed, is provided through search and display services. As a result, SENTINEL will contain information about individuals pertaining to investigations, and the information can be used to make potential linkages between incidents and investigations. The SENTINEL PIA is available at: http://www.fbi.gov/foia/privacy-impact-assessments/sentinel.

- **DEA's Registrant Information Consolidated System (RICS)**

RICS is a group of applications that collect and maintain information – pursuant to the Controlled Substances Act of 1970 (CSA), as amended, and other authorities – about persons that handle or seek to handle controlled substances and listed chemicals. The CSA and its implementing regulations generally make it unlawful to manufacture, distribute, dispense, or possess controlled substances or List I chemicals except in an authorized manner. Those that seek to handle controlled substances or List I chemicals must obtain a registration from the Attorney General. RICS automates application, registration, compliance, and reporting, and it

supports investigation and enforcement efforts. The RICS PIA is available at: http://www.justice.gov/dea/FOIA/pia_docs/rics_%20pia_060414.pdf.

B. SYSTEM OF RECORDS NOTICES REVIEWS

During the reporting period, the Department of Justice completed and published one System of Records Notice (SORN) for the Office on Violence Against Women (OVW). A system of records is defined by the Privacy Act of 1974 as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. § 552a(a)(5). Agencies are required to publish in the Federal Register notice of any new use or intended use of the information in the system of record.

OPCL submitted to the Federal Register for publishing a notice of a new system of records titled, "Peer Reviewer Database", JUSTICE/OVW–001 (79 Fed. Reg. 28774). The Peer Reviewer Database (Database) allows OVW to select individuals who have expressed interest in serving as peer reviewers for reviewing grant applications during the solicitation process for different federal grant programs authorized by the Violence Against Women Act, as amended, and administered by OVW. These grant programs enable communities to increase their capacity to respond to crimes of domestic violence, dating violence, sexual assault, and stalking. As part of the review process, prior to making award decisions, OVW may assemble different peer review panels to review and score the applications received in response to a solicitation for a particular grant program. These peer review panels are comprised of experts and practitioners, on the subject matter pertaining to the grant, who review and score grant applications based on the requirements outlined in the solicitation for that particular grant program. Records are collected on those individuals who are selected by OVW to serve as peer reviewers, as well as individuals who are candidates to be a peer reviewer. The Peer Reviewer Database SORN is available at: http://www.justice.gov/opcl/doj-systems-records. This SORN is a companion to the above listed PIA for OWV's Peer Reviewer Database that is available at: http://www.justice.gov/sites/default/files/opcl/docs/ovw-pia-peer-review-database.pdf.

III. 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 quarter, the CPCLO or OPCL did not provide any formal written guidance.

For this quarter, OPCL provided live presentations on privacy issues and protections at two Department conferences:

- OVW's Summit on the Workplace Impact of Domestic and Sexual Violence and Stalking.
- DOJ's Office of Chief Information Officer Information Technology Conference.

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

- Meeting with Privacy Advocates: The CPCLO and OPCL met with privacy advocates to discuss the Department's privacy initiatives and provided an overview of the Department's privacy compliance program. In addition, the CPCLO and OPCL met with privacy advocates to discuss the Big Data Report published by the Executive Office of the President, led by John Podesta, Counselor to the President.
- OPCL met with Cultural Vistas and European delegates under the auspices of the U.S. Department of State's International Visitor Leadership Program (IVLP) to discuss transparency of federal government operations and the Department's privacy initiatives and Department's privacy compliance program. Cultural Vistas is a non-profit organization that has facilitated professional exchange programs and services for visitors coming to the United States, and Americans seeking overseas experiential learning opportunities. As one of seven National Program Agencies (NPAs), Cultural Vistas works in close cooperation with the U.S. Department of State to administer, design, and implement IVLP programs that directly support and advance U.S. foreign policy goals.
- The CPCLO and OPCL continued to meet with the European Delegation regarding E.U. and U.S. Data Protection and Privacy Agreement (DPPA) negotiations. For instance, the CPCLO participated in a negotiation session of the DPPA on May 22 - 23, 2014, in Brussels, Belgium.
- The CPCLO participated on a panel titled "Big Data and Discrimination" as part of a workshop titled "Improving Government Performance in the Era of Big Data: Opportunities and Challenges for Federal Agencies." This workshop was hosted by the White House's Office of Science and Technology Policy (OSTP) and the Georgetown University McCourt School of Public Policy's Massive Data Institute. The panel addressed the potential discriminatory effects from the collection and use of big data by federal government agencies.

IV. 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.

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[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 Third Quarter of Fiscal Year 2014, OPCL received 86 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 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.