U.S. Department of Justice - Federal Bureau of Investigation

THE PRIVACY AND CIVIL LIBERTIES OFFICER AND THE PRIVACY AND CIVIL LIBERTIES UNIT

PRIVACY AND CIVIL LIBERTIES ACTIVITIES SEMI-ANNUAL REPORT

SECOND SEMI-ANNUAL REPORT, FY 2023

APRIL 1, 2023 – SEPTEMBER 30, 2023

I. INTRODUCTION

Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, 42 U.S.C. § 2000ee-1 (2018) (hereinafter "Section 803"), requires designation of a senior officer to serve as the Federal Bureau of Investigation (FBI) Director's principal advisor on privacy and civil liberties matters and imposes reporting requirements on certain activities of this officer.[1] The FBI's Privacy and Civil Liberties Officer (PCLO) in the FBI's Office of the General Counsel serves as this senior officer, and is supported by the FBI's Privacy and Civil Liberties Unit (PCLU).

Specifically, Section 803 requires periodic reports related to the discharge of certain privacy and civil liberties functions of the FBI's PCLO, including information[2] on: (1) the number and types of privacy reviews undertaken; (2) the type of advice provided and the response given to such advice; (3) the number and nature of complaints received by the FBI for alleged violations; and (4) a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of this officer.

II. PRIVACY REVIEWS

Section 803 requires the inclusion of "information on the number and types of reviews undertaken" in this Semi-Annual Report.[3] Among these are the reviews the FBI 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, as amended, 5 U.S.C. § 552a (2018) (Privacy Act); the privacy provisions of Section 208 of the E-Government Act of 2002 (E-Government Act), 44 U.S.C. § 3501 (note) (2018); and federal privacy policies articulated in the U.S. Office of Management and Budget (OMB) guidance, including OMB Circular A-130.[4] Regular reviews conducted within the requirements of Section 803 include the following:

1. Privacy Threshold Analyses (PTAs):

A PTA is a privacy compliance tool developed by the FBI as a first step to: (1) facilitate the identification of potential privacy issues; (2) assess whether additional privacy documentation is required; and (3) ultimately ensure the FBI's compliance with applicable privacy laws and policies. All information systems must have PTAs. PTAs are prepared by the applicable program management and Division Privacy Officers in coordination with PCLU. The FBI

---

[1] The Foreign Intelligence Surveillance Act (FISA) Amendments Reauthorization Act of 2017, Section 109, amended the Intelligence Reform and Terrorism Prevention Act of 2004 (Section 803) to add the FBI Director to the list of Executive Branch leaders required to designate senior privacy and civil liberties officers and periodically report on certain activities of such officers. *See* The FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, § 109, 132 Stat. 3, 15 (2018).
[2] The FBI's numbers include the FBI's Privacy Impact Assessments listed in DOJ's Section 803 Report for this reporting period.
[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://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf.

PCLO approves all PTAs. For purposes of this report, this number represents PTAs approved by the PCLO.

2. **Other Privacy Reviews**

Data Ingest Privacy Reviews (DIPRs), Cloud Legal and Privacy Reviews (CLPRs), and Routine Database Checklists are additional privacy compliance tools. DIPRs were developed by the FBI to help assess and document the privacy risks associated with the ingestion of new types of data into existing FBI information systems that are already covered by PTAs. CLPRs were developed by the FBI to assess and document privacy risks associated with transferring existing, appropriately documented FBI information systems or datasets to cloud environments. The Routine Database Checklist was developed by the FBI, as a standardized approach for simple systems containing routine information and involving limited use and access.[5] DIPRs, CLPRs, and Routine Database Checklists are prepared by the applicable program management and Division Privacy Officers in coordination with PCLU. The FBI PCLO approves all DIPRs, CLPRs, and Routine Database Checklists. For purposes of this report, the category of "other privacy reviews" includes the number of DIPRs, CLPRs, and Routine Database Checklists approved by the PCLO.

3. **Privacy Impact Assessments (PIAs):**

A PIA is an analysis, required by Section 208 of the E-Government Act, of how information in identifiable form is processed to: (1) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[6] Under the E-Government Act, PIAs are not required for national security systems, but the FBI still completes them, as a matter of Department of Justice (DOJ) policy. All FBI PIAs are completed by FBI program management in coordination with PCLU and are reviewed and conditionally approved by the FBI's PCLO and Chief Information Officer (CIO). The PCLU then forwards FBI approved PIAs to the DOJ's Office of Privacy and Civil Liberties (OPCL) and Chief Privacy and Civil Liberties Officer (CPCLO) for final approval. For purposes of this report, this number represents PIAs approved by FBI's PCLO and DOJ's CPCLO.

---

[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.C.6.b.3 ("Routine database systems") (Sept. 26, 2003), https://www.whitehouse.gov/wp-content/uploads/2017/11/203-M-03-22-OMB-Guidance-for-Implementing-the-Privacy-Provisions-of-the-E-Government-Act-of-2002-1.pdf.

[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://www.whitehouse.gov/wp-content/uploads/2017/11/203-M-03-22-OMB-Guidance-for-Implementing-the-Privacy-Provisions-of-the-E-Government-Act-of-2002-1.pdf.

4. **System of Records Notices (SORNs):**

A SORN is a notice required by the Privacy Act that describes the existence and character of systems 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] SORNs are published in the Federal Register. FBI SORNs are written by PCLU in coordination with FBI program management. They are then reviewed and approved by FBI's PCLO and reviewed and approved by DOJ's OPCL and CPCLO. For purposes of this report, this number represents SORNs reviewed and approved by FBI's PCLO, OPCL, and CPCLO that resulted in published SORNs for which the comment periods have closed.

5. **Privacy Act Exemption Regulations:**

The Privacy Act provides that agencies may exempt some systems of records from certain provisions of the Privacy 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 Privacy Act.[8] For purposes of this report, this number represents published FBI Privacy Act exemption regulations that have resulted in final rules that have taken effect.

6. **Data Breaches or Incidents:**

DOJ Instruction 0900.00.01, *Reporting and Response Procedures for a Breach of Personally Identifiable Information*,[9] defines a breach as:

> [T]he 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 "[a]n occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or 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, including the FBI, and contractors who operate systems supporting DOJ. Additionally, FBI Policy Directive 0504D, *Roles and Responsibilities*

[7] *See* 5 U.S.C. § 552a(e)(4).
[8] *See id.* § 552a(j), (k).
[9] *See* DOJ Instruction 0900.00.01, *Reporting and Response Procedures for A Responsibilities for Managing Breach of Personally Identifiable Information* (Feb. 16, 2018). On November 17, 2023, this Instruction was cancelled by DOJ Policy Statement 0904.02, *Incident and Breach Response Playbook*. However, we are citing this Instruction as it was in effect during this reporting period.

for Reporting a Data Breach is applicable, which is consistent with this instruction.[10] For purposes of this report, this number includes FBI data breaches and incidents that have been formally reviewed by DOJ's Core Management Team (DOJ's organizational team chaired by the DOJ's CPCLO and Chief Information Officer, which convenes in the event of a significant data breach involving PII).

PRIVACY REVIEWS[11]	
Type of Review	**Number of Reviews**
PTAs	94
Other Privacy Reviews: DIPRs, CLPRs, and Routine Database Checklists	9
PIAs[12] • Next Generation Identification Biometric Interoperability • Financial Reporting Application • eFile and Entellitrak	7
SORNs[13]	0
Privacy Act Exemption Regulations	0
Data breach and/or incident reviews	0

III. <u>ADVICE</u>

Section 803 requires the inclusion of information regarding "the type of advice provided and the response given to such advice" in this Semi-Annual Report.[14] The PCLO'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. This advice has been drafted or authorized by the PCLO 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 PCLO received appropriate responses to the formal and informal advice provided.

[10] On September 11, 2024, the Data Breach Reporting and Response Policy Directive, 1335D, was published, which supersedes the cited policy. However, we have continued to cite to the older policy as it was in effect during this reporting period.
[11] The FBI's PIA and SORN numbers include those listed in DOJ's Section 803 Report for this reporting period.
[12] FBI PIAs, https://www.fbi.gov/services/information-management/fioapa/privacy-impact-assessments. Note: four of the PIAs included in the number of reviews have not been listed because of the sensitivity of the associated systems.
[13] FBI SORNs, https://www.justice.gov/opcl/doj-systems-records.
[14] *See* 42 U.S.C. § 2000ee-1(f)(2)(B).

During this reporting period, the PCLO and PCLU provided formal and informal advice on various matters with privacy and civil liberties implications including, but not limited to the following topics:

1. FBI's compliance with laws, regulations, and policies relating to information privacy, such as the Privacy Act, Section 208 of the E-Government Act, and the Federal Information Security Modernization Act;
2. Best practices to achieve an appropriate balance between protecting civil liberties while facilitating FBI investigative and intelligence collection activities;
3. Development, evaluation, and implementation of legislative, regulatory, and other policy proposals to ensure that privacy and civil liberties issues are adequately considered and addressed;
4. Periodic investigation and review of FBI actions, policies, procedures, and guidelines to ensure that privacy and civil liberties issues are adequately considered and addressed;
5. Coordination of FBI responses to privacy-related audits, oversight engagements, and reviews;
6. Creation, acquisition, or modification of information systems, datasets, software as a service, and tools;
7. Collection, maintenance, and use of biometric information, including facial recognition technology;
8. Operational and administrative activities involving the collection or disclosure of PII or information regarding the exercise of First Amendment rights, including the use of social media tools and commercially available information;
9. Evaluation of commercial applications for privacy equities on enterprise mobile devices;
10. Issuance, revision, and administration of privacy and civil liberties-related education and trainings to help ensure FBI-wide compliance with privacy and civil liberties mandates;
11. Initiation or modification of information sharing activities;
12. Participation in FBI, DOJ, and Intelligence Community working groups concerning privacy and civil liberties matters; including emerging technologies such as commercially available information, artificial intelligence, and facial recognition technology;
13. Review of congressional taskings concerning privacy and civil liberties matters;
14. Compliance with the First Amendment and other civil liberties protections;
15. Creation and/or revision of FBI consent forms;
16. Research projects with human subjects;
17. Provision of watchlisting guidance to the Terrorist Screening Center;
18. Requests to deploy unmanned aircraft systems;
19. Insider threat matters; and
20. National Vetter Center (NVC) initiatives.

With regard to insider threat matters, the PCLU has been an active member of the DOJ Insider Threat Working Group pursuant to DOJ Order 0901, which established the DOJ Insider Threat Prevention and Detection Program (ITPDP) and mandated that the ITPDP "include appropriate protections for legal, privacy, civil rights, and civil liberties requirements." PCLU is also an active member of the NT-50 Insider Threat Legal Community of Practice.

Additionally, the PCLO and PCLU participated in NVC initiatives such as the National Vetting Governance Board Steering Committee and the Privacy, Civil Rights, and Civil Liberties Working Group, advising on privacy and civil liberties issues.

IV. COMPLAINTS[15]

Section 803 requires the inclusion of "the number and nature of the complaints received by the department, agency, or element concerned for alleged violations" in this Semi-Annual Report.[16] Privacy complaints encompass written allegations (excluding complaints filed in litigation against the FBI) concerning violations of privacy protections in the administration of the programs and operations of the FBI that are submitted to or through the PCLO,[17] PCLU,[18] the Record/Information Dissemination Section of the FBI Information Management Division (RIDS),[19] the Office of Integrity and Compliance (OIC),[20] or FBI Headquarters Division and Field Office Privacy Officers (Division Privacy Officers). Complaints received by other FBI divisions, sections, units, and offices without notice to the PCLO, PCLU, RIDS, OIC, or a Division Privacy Officer are handled by those divisions, sections, units, and office and are not counted for purposes of this report. Privacy complaints can be 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); and
3. Operational issues (inquiries regarding general privacy, including Privacy Act matters).

Civil liberties complaints encompass written allegations (excluding complaints filed in litigation against the FBI) for problems with or violations of civil liberties safeguards concerning the handling of personal information by the FBI in the administration of FBI programs and operations that are submitted to or through the PCLO, PCLU, RIDS, OIC, or Division Privacy Officers. Complaints received by other FBI divisions, sections, units, and offices without notice to the PCLO, PCLU, RIDS, OIC, or a Division Policy Officer are handled by those divisions, sections, units, and office and are not counted for purposes of this report.

---

[15] This number is not included in DOJ's Section 803 Report for this reporting period.
[16] *See* U.S.C. § 2000ee-1(f)(2)(C).
[17] On March 22, 2022, a Complaints section was added to the FBI Privacy Policy webpage at www.fbi.gov/privacy-policy. This webpage advises the public that complaints of privacy and civil liberties violations in connection with the FBI's handling of information may be mailed to the FBI, Attn: Privacy and Civil Liberties Officer, 935 Pennsylvania Avenue NW, Washington, D.C. 20535-0001.
[18] On March 1, 2022, a Privacy and Civil Liberties Complaints section was added to PCLU's internal webpage titled "About Us."
[19] RIDS is responsible for records requests under the Freedom of Information Act, 5 U.S.C. § 552, and the Privacy Act.
[20] OIC is an FBI Division that is responsible for, among other things, ensuring there are processes and procedures in the FBI that promote compliance with all laws, regulations, and rules governing operations, programs, and activities.

For each type of privacy or civil liberties complaint received by the PCLO, PCLU, RIDS, OIC, or Division Privacy Officers during the reporting period, this report includes categories for 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 reporting period, the complaint may be counted and addressed in the subsequent reporting period if time constraints hinder a thorough examination of the complaint in the reporting period in which it is received.

Privacy and Civil Liberties Complaints			
Type of Complaint	**Number of Complaints**	**Disposition of Complaint**	
		Referred to another FBI division or field office for review	**Referred to Inspection Division or DOJ Office of Inspector General**
Process and Procedure	0	0	0
Redress	0	0	0
Operational	0	0	0
Civil Liberties Complaints	0	0	0
Total	0		

V. INFORMING THE PUBLIC

Pursuant to Section 803, the PCLO 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."[21] During the reporting period, the PCLO and PCLU have engaged stakeholders in the FBI, DOJ, Intelligence Community, and external privacy community. The PCLO and PCLU also participated in multiple speaking engagements to promote transparency of the FBI's policies, initiatives, and oversight with respect to the protection of privacy and civil liberties.

VI. OTHER FUNCTIONS

Throughout the reporting period, the PCLO has worked with the Privacy and Civil Liberties Oversight Board to address privacy concerns, and ways to improve agency outreach. Moreover, the PCLO and PCLU have met with other Federal agencies to improve inter-agency coordination, and to discuss agency privacy practices and common concerns. These meetings enable the PCLO and PCLU to review and assess the FBI's information and privacy-related policies and make improvements where appropriate and necessary.

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