U.S. Department of Justice **0601**

Approved On: May 14, 2020

DOJ ORDER

PRIVACY AND CIVIL LIBERTIES

PURPOSE:	Establishes the responsibilities of the Chief Privacy and Civil Liberties Officer, Senior Component Officials for Privacy, the Office of Privacy and Civil Liberties, and the Heads of Components for privacy and civil liberties matters in the Department of Justice ("DOJ" or "Department")
SCOPE:	All DOJ components
ORIGINATOR:	Chief Privacy and Civil Liberties Officer
CATEGORY:	(I) Administrative, (II) Information and Privacy
AUTHORITY:	Section 1174 of the Violence Against Women and DOJ Reauthorization Act of 2005, Pub. L. No. 109-162 (Jan. 5, 2006) (codified at 28 U.S.C. § 509 note); Section 803(a) of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53 (Aug. 3, 2007) (codified at 42 U.S.C. § 2000ee-1), as amended by Section 109 of the FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118 (Jan. 19, 2018) (codified at 42 U.S.C. § 2000ee-1); 28 U.S.C. §§ 503, 504, 510; 28 C.F.R. §§ 0.5, 0.15; Office of Management and Budget Memorandum for Heads of Executive Departments and Agencies M-16-24, *Role and Designation of Senior Agency Officials for Privacy* (Sept. 15, 2016)
CANCELLATION:	Order DOJ 3011.1A
DISTRIBUTION:	Electronically distributed to those referenced in the "SCOPE" section and posted on the DOJ directives electronic repository (SharePoint) at: [redacted]

APPROVED BY: *Jeffrey A. Rosen*
Deputy Attorney General

ACTION LOG

All DOJ directives are reviewed, at minimum, every 5 years and revisions are made as necessary. The action log records dates of approval, recertification, and cancellation, as well as major and minor revisions to this directive. A brief summary of all revisions will be noted. In the event this directive is cancelled, superseded, or supersedes another directive, that will also be noted in the action log.

Action	Authorized by	Date	Summary
Initial Document Approval	James M. Cole Deputy Attorney General	2-6-2014	Sets forth roles and responsibilities of the Department's CPCLO, OPCL, Heads of Components, and SCOPs regarding privacy and civil liberties.
Revisions	Jeffrey Rosen, Deputy Attorney General	5-14-2020	Revisions reflect new legislative requirements, and Office of Management and Budget guidance. In addition, revisions were made to the roles and responsibilities of the Department's Chief Privacy and Civil Liberties Officer, Office of Privacy and Civil Liberties, Heads of Components, and Senior Component Officials for Privacy.

TABLE OF CONTENTS

DEFINITIONS

Term	Definition
Data Breach	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition; or any similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.
Fair Information Practice Principles	Information governance principles that were developed in the 1970s, used in the Privacy Act of 1974, and other federal laws and policies. These laws and policies require agencies to disclose their purposes for collecting personal information, limit collection to what is needed, control its use for secondary purposes, allow affected individuals to access it and correct inaccuracies, as well as keep it secure.
Personally Identifiable Information	A broad term for information that can be used to distinguish or trace an individual's identity, alone or when combined with other information that is linked or linkable to a specific individual.
Privacy Act Record	Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to a person's education, financial transactions, medical history, and criminal or employment history and that contains a person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

ACRONYMS

Acronym	Meaning
CPCLO	Chief Privacy and Civil Liberties Officer
FIPPs	Fair Information Practice Principles
FISMA	Federal Information Security Modernization Act
ISE	Information Sharing Environment
OPCL	Office of Privacy and Civil Liberties
PII	Personally Identifiable Information
SAOP	Senior Agency Official for Privacy
SCOP	Senior Component Official for Privacy

I. Policy

This Order reaffirms the longstanding commitment of the Department of Justice (DOJ or Department) to the protection of privacy and civil liberties by setting forth roles and responsibilities of key positions and offices responsible for the Department's compliance with the laws, regulations, and established policies designed to protect the privacy of individuals.

It is the policy of the Department to appropriately consider concerns regarding privacy and civil liberties in the development and implementation of legislative, regulatory, and other policy proposals related to efforts to defend the nation against terrorism, protect national security and public safety, and enforce laws.

In carrying out its mission to enforce the law and defend the interests of the United States, the Department understands the importance of protecting the privacy and civil liberties of persons, including the proper handling of Personally Identifiable Information (PII). Consistent with applicable laws, regulations, and mission needs, the Department will, as appropriate, consider the Fair Information Practice Principles (FIPPs) in Department and component-level privacy policy development and implementation, and when reviewing programs, systems, or operations that raise privacy issues or concerns. The FIPPs foster mutual trust between agencies and individuals around a shared commitment to the integrity of the information used in agency decision-making.[1] They are also helpful guides when analyzing risks involved in the operation of information systems.[2]

In adversarial matters involving civil litigation, and in connection with criminal law enforcement or national security, full application of the FIPPs may not be appropriate. In these contexts, the Department will continue to develop and apply the practices and procedures it has pioneered to properly manage and protect sensitive personal information as it carries out its mission. These include the practices and procedures found in the Attorney General's Guidelines under Section 2.3 of Executive Order 12333, the Justice Manual (formerly known as the United States Attorney's Manual), and the Federal Bureau of Investigation (FBI) Domestic Investigations and Operations Guide. Consistent with the purpose of the FIPPs to maintain trust, these alternative practices and procedures provide an information governance framework designed to ensure DOJ employees legally, effectively, and efficiently execute authorized Department functions, while mitigating risks to privacy and civil liberties. The Department's authority to collect and use personal information is critical to the Department's mission, and this in turn depends on its ability to maintain the trust of the American people.

II. Roles and Responsibilities

A. Chief Privacy and Civil Liberties Officer

1. Designation of Chief Privacy and Civil Liberties Officer

The Chief Privacy and Civil Liberties Officer (CPCLO) is designated by the Attorney General and reports to the Deputy Attorney General as a member of the Office of the Deputy Attorney General.[3] The Attorney General may designate a

[1] *See* RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS, REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, U.S. Department of Health, Education and Welfare (July, 1973).
[2] *See* Section 208 of the E-Government Act of 2002, 44 U.S.C. § 3501, note.
[3] Although Section 2000ee-1(c) of Title 42, United States Code, provides that the CPCLO "will report directly to the head

non-career Senior Executive Service officer as the CPCLO, or may select a member of the career Senior Executive Service. In the absence of an appointed CPCLO, the Director of Office of Privacy and Civil Liberties (OPCL) serves as the Acting CPCLO of the Department, and the Deputy Director of OPCL as the Acting Director of OPCL. As appropriate, unless otherwise limited by law, the CPCLO may delegate specific responsibilities of the CPCLO to the Director of OPCL, to a Senior Component Official for Privacy (SCOP), or to another Department official who has the necessary skills and expertise to perform the delegated responsibilities, subject to the CPCLO's oversight.

2. **Statutory Duties**

Pursuant to statute, the CPCLO is the principal advisor to Department leadership and components on privacy and civil liberties matters affecting the Department's missions and operations, and fulfills the statutory duties set forth in Section 1174 of the Violence Against Women and DOJ Reauthorization Act of 2005, and Section 803 of the 9/11 Commission Act. The CPCLO has primary responsibility for the Department's privacy policy, and is to consider the privacy and civil liberties implications of proposed or existing laws, regulations, procedures, and guidelines. The CPCLO also has primary responsibility for the Department's compliance with the Privacy Act of 1974; the E-Government Act of 2002; Federal Information Security Modernization Act; and all other privacy laws, regulations, policies, and directives protecting the personal information of individuals.

3. **Senior Agency Official for Privacy**

a. The Department's CPCLO also fulfills the role of Senior Agency Official for Privacy (SAOP). Pursuant to the Office of Management and Budget (OMB) directives, a SAOP is the senior official, designated by the agency head, with agency-wide responsibility and accountability for its privacy program, including implementation of privacy protections; compliance with privacy related federal laws, regulations, and policies; management of privacy risks; and playing a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals affecting privacy. OMB requires the SAOP to be a senior official with necessary skills, knowledge, expertise, and authority, serving in a central leadership position, with visibility into relevant agency operations, and regularly engaging with agency leadership, including the head of the agency.[4]

b. In order for the CPCLO to perform his/her duties, the CPCLO must have access to information, material, resources, and personnel necessary to carry out his/her functions and be able to coordinate activities with the DOJ Office of the Inspector General, as appropriate.

---

of the department," the Attorney General has delegated this reporting function to the Deputy Attorney General, consistent with the reporting structure of other Heads of Components. *See* Deputy Attorney General Order No. 0601, Privacy and Civil Liberties (Feb. 6, 2014).

[4] OMB Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy* (2016), at 2; *see also* OMB Circular A-130, app. II at 3-4.

c. **Specific Responsibilities of the Chief Privacy and Civil Liberties Officer**

1. The CPCLO is responsible for:

a. Maintaining a privacy program plan that provides an overview of the DOJ privacy program, including a description of the structure of the DOJ privacy program, the resources dedicated to the privacy program, the role of the CPCLO and other privacy officials and staff, the strategic goals and objectives of the privacy program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.

b. Ensuring that the Department considers appropriate privacy protections in the collection, storage, use, dissemination, and security of PII, along with managing privacy risks throughout the information lifecycle, with respect to the Department's existing or proposed information technology (IT) and information systems, consistent with applicable information governance frameworks.[5]

c. Evaluating for potential privacy and civil liberties impacts, all Department-wide programs and initiatives, as well as programs and initiatives with which the Department may participate with other agencies, and advising Department leadership and components on implementing corresponding privacy and civil liberties protections.

d. Overseeing and maintaining primary responsibility over the Department's compliance with the Privacy Act and other applicable privacy laws and regulations, and policy directives of the Department or the OMB.

e. Reviewing policies, procedures, or programs to ensure that concerns about privacy and civil liberties have been appropriately addressed in connection with the design and operation of such policies, procedures or programs in conjunction with the National Security Division, the FBI, or other appropriate components.

f. Developing and implementing policies and practices designed to eliminate unnecessary collection, maintenance, and use of Social Security numbers, and exploring alternatives to the use of Social Security numbers as a personal identifier.

g. Providing and issuing Department-wide advice, guidance, policy, and procedures on issues concerning the interpretation, application, and implementation of privacy policies and privacy compliance matters.

h. Reviewing and approving Department privacy compliance documentation.

[5] *See*, *e.g.*, The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (Oct. 31, 2003) (https://fas.org/irp/agency/doj/fbi/nsiguidelines.pdf).

i. Ensuring that the Department meets privacy reporting requirements.

j. Coordinating and referring appropriate review of and responses to complaints and inquiries regarding possible violations of privacy and civil liberties.

k. Adjudicating appeals of denials of requests to amend records submitted pursuant to the Privacy Act.

l. Reviewing privacy and civil liberties implications of legislative and regulatory proposals and guidelines affecting the Department and involving the collection, storage, use, disclosure, and security of PII.

m. Developing, maintaining, and providing DOJ-wide privacy awareness and training programs to ensure that personnel have the appropriate knowledge and skill to comply with law, mitigate privacy risks, properly safeguard privacy interests, and establishing rules of behavior and other accountability measures for employees and contractors with access to PII.

n. Overseeing the Department's responses to data breaches in coordination with the Chief Information Officer (CIO).

o. Ensuring that adequate resources and staff are devoted to meeting the Department's privacy-related functions and obligations, and analyzing IT investment plans and budgetary requests to ensure they meet privacy requirements, address privacy risks, and include adequate resources for privacy risk mitigation.

p. Developing and implementing workforce planning processes to ensure that DOJ can anticipate and respond to changing mission requirements, maintain workforce skills in a rapidly developing IT environment, and recruit and retain the privacy talent needed to accomplish the Department's missions.

q. Serving as the Department's SAOP and its representative on the Federal Privacy Council; the Department's Information Sharing Environment (ISE) Privacy Official; Co-Chair of the Department's data breach Core Management Team; a member of the Department's Data Integrity Board; a member of the Watchlisting Advisory Council; and an ex officio member of the FBI's Special Operations Review Committee; the National Domestic Communications Assistance Center; and the Global Advisory Committee; and as an advisor to other agency organizations from time to time as required by law or policy.

r. No later than the end of each fiscal year, collaborate with each SCOP regarding: (1) the need for updates to current DOJ or component privacy policies and procedures, training, and privacy program

resource allocations; (2) the current status of the component's compliance documentation and whether compliance goals for the prior fiscal year were achieved; and (3) the components' compliance goals for the next fiscal year, including applicable metrics.

s. At least annually, the CPCLO will provide feedback to the Heads of Components or other appropriate official in its leadership,[6] with an assessment of the performance of the component's privacy program.

B. Heads of Components

1. After consultation with the CPCLO, the Heads of Components must designate a SCOP, who will have the responsibilities and duties described in Part C of this Order. The SCOP will serve as the CPCLO's and OPCL's main point of contact concerning privacy matters (e.g., implementing privacy rules, regulations, policies, and laws, mitigating privacy risks in information systems, and responding to breaches). In choosing a SCOP, the Heads of Components should consider individuals who possess experience and background in privacy law and policy, and who will be accountable for the component's privacy matters. The Heads of Components must ensure that SCOPs receive adequate training, support, and resources to complete their duties effectively.

2. Heads of Components must also ensure that their component, through the designated SCOP, consults with the CPCLO when considering new information systems or technologies to ensure appropriate privacy protections are established and maintained for such systems and technologies; as well as to ensure compliance with the Department's legal obligations under the Privacy Act and other statutes, regulations, procedures, and guidelines.

C. Senior Component Officials for Privacy

1. A component's SCOP holds primary responsibility for the applicable component's privacy and civil liberties activities, including compliance with applicable privacy laws, regulations, directives, and policies. SCOPs are responsible at the component level for managing the implementation of privacy laws, regulations, and policies, while the CPCLO maintains overall responsibilities and oversight for the entire Department. Because SCOPs cannot manage such implementation on their own, in performing their responsibilities, SCOPs must collaborate with appropriate DOJ and component level personnel.

2. The Foreign Intelligence Service Act Amendments Reauthorization Act of 2017, § 109, Pub. L. No. 115-118, 132 Stat. 3, 15 (2018) (codified at 42 U.S.C. § 2000ee-1) established certain roles and responsibilities of the FBI Privacy and Civil Liberties Officer (PCLO), who is also the FBI's SCOP. This Order fully applies to the FBI and the FBI SCOP, like all other Department components. In recognition, however, of the statutory roles and responsibilities of the FBI PCLO the CPCLO may exercise his or her authority as CPCLO to further define the relationship as appropriate between the

[6] A designee for this purpose must not be the SCOP.

PCLO and the CPCLO in separate documentation.

3. The Senior Component Officials for Privacy are responsible for:

   a. Implementing DOJ privacy policies and procedures established by Department leadership, the CPCLO, and/or OPCL; and, as necessary, developing component-level privacy policies and procedures for component leadership approval, and implementing such policies and procedures consistent with those at the Department level.

   b. Supporting the CPCLO and OPCL by overseeing the component's compliance with privacy laws and policies, and privacy policy directives of the Administration and the Department in coordination with the CPCLO and OPCL as appropriate.

   c. Managing privacy risks throughout the information lifecycle, with respect to the component's existing or proposed IT and information systems.

   d. Advising the Heads of Components as to whether adequate resources and staff in the component are devoted to meeting the component's privacy-related functions and obligations, and in coordination with the component's CIO or equivalent, analyzing the component's IT investment plans and budgetary requests to advise component heads on whether they meet privacy requirements and address privacy risks, including the costs and resources for privacy risk mitigation.

   e. Ensuring the proper and timely preparation and completion of required privacy compliance documentation.

   f. Coordinating component responses to privacy audits, reviews, and reporting requirements.

   g. Developing as necessary, maintaining, and providing component-level privacy awareness training programs designed to ensure that personnel have the appropriate knowledge and skill to comply with the law, mitigate privacy risks, properly safeguard individual privacy interests, and establish rules of behavior and other accountability measures for employees and contractors, in coordination with the CPCLO and OPCL.

   h. Identifying privacy issues, concerns, or risks, and working with the CPCLO or OPCL to take appropriate steps to address and resolve them.

   i. Reviewing and responding to privacy and civil liberties complaints and redress inquiries, as appropriate.

   j. Ensuring the control and protection of PII through appropriate security measures, privacy controls, and minimization efforts.

   k. Ensuring compliance with applicable departmental procedures in the event of a data breach, including co-chairing the Component Level Management Team when applicable.

   l. Serving as the component ISE Privacy official, as applicable.

m. Advising component leadership on the development and implementation of any component-level policies, procedures, or practices having a significant impact on privacy or civil liberties.

n. Collaborating with the CPCLO regarding: (1) the need for updates to current DOJ or component privacy policies and procedures, training, and privacy program resource allocations; (2) the current status of the component's compliance documentation and whether compliance goals for the prior fiscal year were achieved; and (3) the components' compliance goals for the next fiscal year, including applicable metrics, no later than the end of each fiscal year.