



**DIRECTOR OF ADMINISTRATION AND MANAGEMENT**  
1950 DEFENSE PENTAGON  
WASHINGTON, DC 20301-1950

February 10, 2026

Privacy and Civil Liberties Oversight Board  
800 North Capitol Street, NW  
Suite 565  
Washington, DC 20002

Dear Members of the Board,

Please find enclosed the Department of War Privacy and Civil Liberties Officer Report, pursuant to section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110-53), as amended (42 U.S.C. § 2000ee-1). This report reflects activities covering the reporting period for fiscal year 2025, October 01, 2024, through September 30, 2025.

I am sending an identical letter to the appropriate congressional committees.

Sincerely,

*FOR* *Steph Suh*  
Robert G. Salesses

Enclosure:  
As stated

**Department of War**  
**Privacy and Civil Liberties Officer Report**



**Annual Report for Fiscal Year 2025**  
**October 1, 2024 – September 30, 2025**

The estimated cost of this report or study for the Department of War is approximately \$24,000 in Fiscal Years 2025 - 2026. This includes \$0 in expenses and \$24,000 in DoW labor.

Generated on 2026Jan06 RefID: 9-036D9DA

## TABLE OF CONTENTS

I. INTRODUCTION .....	4
II. THE DOW PRIVACY AND CIVIL LIBERTIES PROGRAMS .....	5
A. The Assistant to the Secretary of War for Privacy, Civil Liberties, and Transparency .....	6
B. The Office of the Assistant to the Secretary of War for Privacy, Civil Liberties, and Transparency .....	7
1. The Privacy and Civil Liberties Directorate .....	8
2. The Freedom of Information Act Directorate.....	8
3. The Intelligence Oversight Directorate.....	8
4. The Regulatory Directorate .....	9
5. The Data and Emerging Technologies Directorate.....	9
C. DoW Office of General Counsel.....	10
D. DoW and OSW Component Privacy and Civil Liberties Officials.....	10
1. Senior Component Officials for Privacy .....	10
2. Component Privacy and Civil Liberties Officers .....	11
III. REVIEWS.....	11
A. System of Records Notice Reviews .....	12
B. Exemption Rule Reviews .....	12
C. Matching Agreement Reviews .....	12
D. Privacy Breach Reviews .....	13
E. Social Security Number Justification Reviews .....	13
F. DoW Issuances, Federal Legislation, Testimonies, and Reports .....	13
<b>Table 1: Privacy and Civil Liberties Reviews from October 1, 2024, to September 30, 2025</b> .....	14
IV. MATTERS OF ADVICE AND ACHIEVEMENTS .....	14
A. Advice .....	14
B. Programmatic Achievements .....	15
V. COMPLAINTS .....	20
A. Complaint Dispositions.....	22
B. Privacy Complaints .....	22
C. Civil Liberties Complaints .....	23

D. Complaints Alleging Violations of Conscience, Moral Principles or Religious Beliefs Under Section 533 of Pub. Law 112-239, as amended .....	23
<b>Table 2: Privacy and Civil Liberties Complaints (received via Privacy and Civil Liberties Program Offices) .....</b>	<b>25</b>
CONCLUSION.....	26
APPENDIX: Samples of Privacy and Civil Liberties Complaints .....	i
Sample DoW Privacy Complaints.....	i
Sample DoW Civil Liberties Complaints.....	i

## I. INTRODUCTION

The Department of War (“DoW” or “Department”) submits this Privacy and Civil Liberties Officer Report (hereinafter referred to as “the Report”) covering the activities of the DoW Privacy and Civil Liberties Officer (DoW PCLO) for fiscal year (FY) 2025: October 1, 2024, through September 30, 2025. Note, in October 2025, the Office of the Assistant to the Secretary of War for Privacy, Civil Liberties, and Transparency (OATSW(PCLT)) was realigned under the Director for Administration and Management. Any changes to the DoW Privacy and Civil Liberties Program resulting from that realignment will be reflected in the next fiscal year’s report. For the purposes of this Report, all activities and accomplishments reflect FY 2025 and align with the organizational structure outlined below.

Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, (Public Law 110-53), codified at 42 U.S.C. § 2000ee-1, requires the Secretary of War to designate a senior officer to serve as the Department’s principal advisor on privacy and civil liberties matters and to report on an annual basis the activities of this officer. During the reporting timeframe, the Assistant to the Secretary of War for Privacy, Civil Liberties, and Transparency (ATSW(PCLT)) served as the DoW PCLO and reported to and advised the Secretary of War and the Deputy Secretary of War on these matters. The Report describes the FY 2025 privacy and civil liberties activities of the DoW, including:

- The organizational structure of the DoW Privacy and Civil Liberties Programs;
- Information on the number and types of reviews undertaken;
- The type of advice provided and the response to such advice;
- The number and nature of the complaints received by the Department for alleged privacy and civil liberties violations; and
- A summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of the DoW PCLO.

The DoW is committed to protecting and promoting privacy and civil liberties in its operations and programs, consistent with the Department’s mission to defend the Nation. In keeping with the Department’s leadership and collaboration in this area, this Report includes the activities of the DoW PCLO in establishing policy and guidelines, as well as the efforts of the

Privacy and Civil Liberties Officials within the DoW and Office of the Secretary of War (OSW) Components who implement these policies.

## **II. THE DOW PRIVACY AND CIVIL LIBERTIES PROGRAMS**

The DoW Privacy and Civil Liberties Programs were established to ensure compliance with the laws, policies, and regulations governing privacy and civil liberties. The DoW PCLO issues and implements DoW privacy and civil liberties policies and directs and oversees the compliance efforts of the DoW Component Privacy and Civil Liberties Programs. The DoW privacy and civil liberties policies and related procedural requirements are established in 32 C.F.R. Part 310, “Protection of Privacy and Access to and Amendment of Individual Records Under the Privacy Act of 1974;” DoD Instruction (DoDI) 5400.11, “DoD Privacy and Civil Liberties Programs,” January 29, 2019, as amended;<sup>1</sup> DoD 5400.11-R, “Department of Defense Privacy Program,” May 14, 2007;<sup>2</sup> DoD Manual (DoDM) 5400.11, Volume 2 “DoD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan,” May 6, 2021, as amended;<sup>3</sup> and DoDI 1000.30, “Reduction of Social Security Number (SSN) Use Within DoD,” August 1, 2012, as amended.<sup>4</sup>

The implementation of the DoW Privacy and Civil Liberties Programs began with the establishment of the Department Privacy Office in 1975, after the passage of Section 552a of Title 5, U.S.C., also known as the Privacy Act of 1974.<sup>5</sup> Following the enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, including Section 803, the Department expanded the mission of the office to fulfill those statutory requirements. As capabilities in information technology and information management continue to become increasingly sophisticated and diverse, the DoW Privacy and Civil Liberties Programs continue to evolve to ensure privacy and civil liberties protections, consistent with the missions of the Department. Figure 1 reflects the structure established through September 30, 2025, for the

---

<sup>1</sup> <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/540011p.pdf>

<sup>2</sup> <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/540011r.pdf>

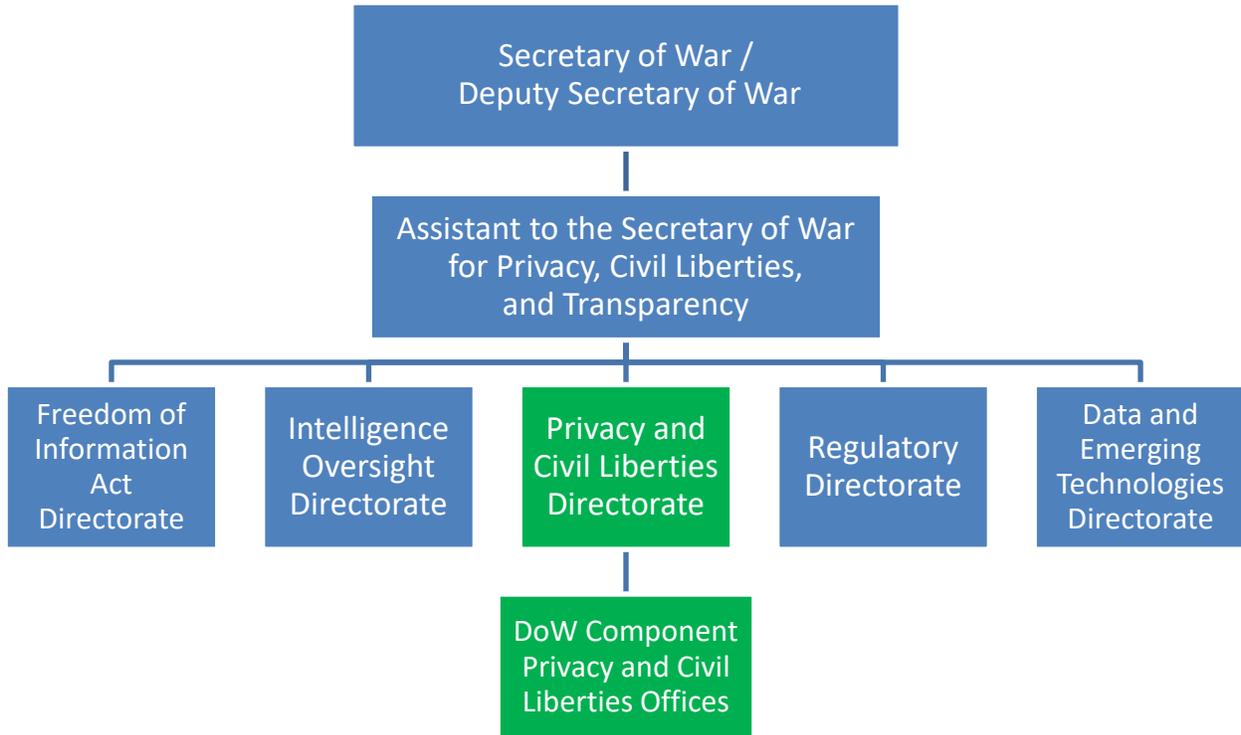
<sup>3</sup> [https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/540011\\_vol2.PDF](https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/540011_vol2.PDF)

<sup>4</sup> <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/100030p.pdf>

<sup>5</sup> The Privacy Act of 1974, 5 U.S.C. § 552a, took effect on September 27, 1975, and can generally be characterized as an omnibus “code of fair information practices” that regulates the collection, maintenance, use, and dissemination of certain records about individuals by Federal executive branch agencies.

DoW Privacy and Civil Liberties programs, including responsible officials and offices within DoW.

**Figure 1: FY25 DoW Privacy and Civil Liberties Programs Structure**



**A. The Assistant to the Secretary of War for Privacy, Civil Liberties, and Transparency**

Consistent with Section 901(b) of the William M. “Mac” Thornberry National Defense Authorization Act (NDAA) for Fiscal Year 2022 (Public Law 116-283), on September 1, 2021, the Deputy Secretary of Defense directed the realignment of the privacy, civil liberties, transparency, regulatory, and intelligence oversight responsibilities under the ATSW(PCLT). The ATSW(PCLT) was also designated as the Principal Staff Assistant responsible for PCLT, regulatory, and intelligence oversight matters.

The ATSW(PCLT) served as the DoW PCLO in accordance with Section 2000ee-1 of Title 42, U.S.C., and reported to and advised the Secretary of War and the Deputy Secretary of

War on privacy and civil liberties issues within the Department's programs and operations. As the DoW PCLO, the ATSW(PCLT) was responsible for ensuring DoW operations, policies, procedures, guidelines, and issuances and their implementation were periodically assessed and updated to provide for the appropriate protection of individuals' privacy and civil liberties. The ATSW(PCLT) was also charged with overseeing the implementation of the Department's Privacy and Civil Liberties Programs, ensuring compliance with the Privacy Act of 1974, as amended, and ensuring appropriate processes were in place to protect individuals' privacy and civil liberties in accordance with the law and policy. The ATSW(PCLT) also engaged with entities charged with the oversight of privacy and civil liberties matters, such as the Privacy and Civil Liberties Oversight Board (PCLOB) and the Office of Management and Budget (OMB).

The ATSW(PCLT) was also designated as the DoW Senior Agency Official for Privacy (SAOP) in accordance with Executive Order 13719, OMB Memorandum M-16-24, OMB Circulars Nos. A-130 and A-108, and DoDI 5400.11. The SAOP has Department-wide responsibility for privacy matters, including the protection of personally identifiable information (PII); compliance with federal privacy-related laws, regulations, and policies; reviewing and providing comments on legislative, regulatory, and other policy initiatives implicating Privacy Act compliance and privacy-related matters; and information privacy risk management. The SAOP sets the parameters and priorities for the DoW Privacy Program. In addition, as DoW's SAOP, the ATSW(PCLT) was actively involved in the Federal Privacy Council, which was established by Executive Order 13719, and served as the Vice Chair to support the protection of privacy across the federal executive branch. The ATSW(PCLT) also participated in key governance structures through which it had the opportunity to assess and advise on privacy and civil liberties concerns.

## **B. The Office of the Assistant to the Secretary of War for Privacy, Civil Liberties, and Transparency**

The OATSW(PCLT) was comprised of five directorates: the Privacy and Civil Liberties Directorate (PCLD), the Freedom of Information Act Directorate (FD), the Intelligence Oversight Directorate (IOD), the Regulatory Directorate (RD), and the Data and Emerging Technologies (DET) Directorate.

### 1. The Privacy and Civil Liberties Directorate

The PCLD supported the ATSW(PCLT) in carrying out responsibilities as the DoW PCLO and SAOP to oversee the implementation of the DoW Privacy and Civil Liberties Programs. This included supporting the ATSW(PCLT) in the following roles: serving as the Chair of the Data Integrity Board and the Privacy Act access and amendment appellate authority for the OSW, the Joint Staff, the Combatant Commands, and other designated components. The PCLD routinely communicated and coordinated on a wide range of activities with DoW and OSW Component privacy and civil liberties officials, the OMB, the PCLOB, and other federal departments and agencies, to facilitate department-wide execution of federal privacy and civil liberties program requirements and to exchange best practices and promote effective and efficient solutions. Also, the PCLD has established reporting processes for the Privacy and Civil Liberties Programs, including the SAOP submission for the annual Federal Information Security Modernization Act (FISMA) (44 U.S.C. Ch. 35, Subch. II) Report; all DoW PII breach reports and notices, including breach notices pursuant to Section 1639(a) of the John S. McCain NDAA for Fiscal Year 2019 (Public Law 115-232) (10 U.S.C. § 2224 note); major incidents involving PII pursuant to FISMA; and this annual PCLO Report.

### 2. The Freedom of Information Act Directorate

The FD assisted the ATSW(PCLT) in carrying out responsibilities as the DoW Chief FOIA Officer pursuant to 5 U.S.C. § 552(j)(1), and as the DoW representative to the Chief FOIA Officers Council pursuant to 5 U.S.C. § 552(k)(1). The ATSW(PCLT) also served as the FOIA appellate authority for the OSW, the Joint Staff, the Combatant Commands, and designated Defense Agencies and DoW Field Activities for information denied under title 5, U.S.C., section 552, and with respect to other adverse determinations.

### 3. The Intelligence Oversight Directorate

The IOD operated under the direction of the DoW Senior Intelligence Oversight Official (SIOO), who also served as the Principal Deputy to the ATSW(PCLT). In accordance with 10 U.S.C. § 430c and DoW policy, the SIOO provides independent oversight of the Department's intelligence and intelligence-related activities, reporting directly to the Secretary of War, as necessary. The IOD independently oversaw all DoW Component's intelligence and intelligence-

related activities to ensure these activities comply with federal law, Executive Orders, Presidential Directives, Intelligence Community directives, and DoW policies. It maintained regular contact with intelligence oversight offices throughout DoW, offering guidance on the implementation of Executive Order 12333. The IOD also oversaw the reporting and remediation of questionable intelligence activities as outlined in DoD Directive 5148.13, compiling quarterly reports for Senior Leaders, the Office of the Director of National Intelligence (ODNI), and the President's Intelligence Oversight Board (IOB). For significant or highly sensitive matters (S/HSMs), the IOD ensured immediate reporting, oversight, and remediation through DoW Senior Leaders, ODNI, and the IOB, as well as follow-on reporting in the IOD quarterly report to the IOB. As an essential partner in the DoW Privacy and Civil Liberties Program, the IOD played a critical role in safeguarding privacy and civil liberties during intelligence and intelligence-related activities.

#### 4. The Regulatory Directorate

Under the direction of the ATSW(PCLT), who served as the designated DoW Regulatory Policy Officer under Executive Order 12866, the RD oversaw the promulgation of all public-facing regulations. The RD served as the Department's Regulatory Lead and e-Rulemaking authority, managing all DoW Regulatory actions and coordinating submission through Regulations.gov, the Federal Docket Management System, and the Office of Information and Regulatory Affairs (OIRA)/OMB. The RD was responsible for reviewing, coordinating, approving, and publishing all DoW rules, notices, and guidance documents that have an impact on the public. This included ensuring compliance with Executive Orders 12866, 13563, 14192, 13132, 13175, and DoW internal requirements. Additionally, the RD managed the Department's regulatory dockets consistent with Section 206 of Public Law 107-347 ("e-Government Act of 2002"). The RD prepared and submitted to OMB the DoW's Regulatory Plan and Regulatory Agenda for inclusion in the Unified Agenda of Regulatory and Deregulatory Actions.

#### 5. The Data and Emerging Technologies Directorate

The DET Directorate supported the Department's mission, enterprise-wide, by assessing and mitigating privacy and civil liberties risks in the use, governance, and oversight of data and emerging technologies; developing and coordinating policy; and enhancing the broader

OATSW(PCLT) mission through innovative technology applications. The DET Directorate engaged Department, interagency, and international partners and collaborated with other key stakeholders to build public trust, mitigate risk for the U.S. government, and set conditions to enhance and support the goals of Department's leadership and the National Defense Strategy. DET Directorate accomplished these tasks by improving organizational performance through aligning key capabilities to high priority concerns, partnering with critical stakeholders to build capabilities, implementation and measuring progress through review of milestones, and applying adjustments as necessary. The DET Directorate concluded operations in FY25 as a result of enterprise-level organizational and workforce posture changes.

### **C. DoW Office of General Counsel**

The DoW Office of General Counsel (OGC) provides legal advice to senior DoW officials and the OATSW(PCLT), and assists DoW and OSW Component legal advisors supporting DoW Privacy and Civil Liberties Programs. In addition, OGC legal advisors worked directly with the OATSW(PCLT) to provide legal reviews of matters implicating privacy and civil liberties issues and to ensure privacy and civil liberties policies were in accordance with the law.

### **D. DoW and OSW Component Privacy and Civil Liberties Officials**

The DoW and OSW Components are responsible for administering their respective Privacy and Civil Liberties Programs, including the establishment and implementation of Component-level privacy and civil liberties policies, procedures, and training consistent with DoW issuances and guidelines. The DoW requires the designation of Senior Component Officials for Privacy (SCOPs) and Component Privacy and Civil Liberties Officers (PCLOs) to lead and implement the various elements of the DoW Privacy and Civil Liberties Programs. The OATSW(PCLT) communicated regularly with these officials on the operation of the Component programs.

#### **1. Senior Component Officials for Privacy**

Each SCOP is typically a general/flag officer, Senior Executive Service, or Senior Level employee. SCOPs oversee the resolution of existing or potential privacy and civil liberties issues

requiring executive-level intervention. They also identify issues and recommend actions for matters requiring the attention of the Component's leadership. In addition, the SCOPs provide information and policy advice to the ATSW(PCLT) to assist in Departmental-level decision-making. The SCOPs also direct Component compliance with Section 803 and the DoW Privacy and Civil Liberties Programs.

## 2. Component Privacy and Civil Liberties Officers

DoW and OSW Components are responsible for designating a Military Service member or civilian employee to serve as the Component PCLO. These officials are responsible for managing the functions of the DoW Privacy and Civil Liberties Programs for the Component organizations. They also collaborate with and assist the SCOPs on all privacy and civil liberties matters as necessary.

### III. REVIEWS

The DoW considers privacy and civil liberties concerns when proposing, developing, and implementing laws, regulations, policies, procedures, and guidelines.<sup>6</sup> Under the direction and guidance of the ATSW(PCLT), the PCLD performed privacy and civil liberties reviews for all Department-level issuances, as well as proposed federal legislation, testimonies, and reports. In doing so, the PCLD analyzed policy, procedures, and activities for their impact on privacy and civil liberties and provided comments and recommended changes to such documents to protect privacy and civil liberties. Upon request, the PCLD reviewed and provided privacy and civil liberties guidance on proposed plans, activities, regulations, policies, and procedures promulgated by other DoW and OSW Components.

Privacy and civil liberties reviews are conducted in accordance with federal laws, such as the Privacy Act of 1974, as amended, certain rights guaranteed in the U.S. Constitution, and OMB and PCLOB executive guidance. The Department also ensures compliance and alignment with FISMA and the E-Government Act of 2002 (44 U.S.C. § 3501 *et seq.*) with respect to information management requirements. For the purposes of this Report, privacy compliance

---

<sup>6</sup> See 42 U.S.C. § 2000ee-1.

reviews are enumerated as follows and are summarized in Table 1.

### **A. System of Records Notice Reviews**

The Privacy Act of 1974 requires that agencies publish a system of records notice (SORN) in the *Federal Register* describing the existence and character of any agency system of records.<sup>7</sup> DoW and OSW Components must submit new, modified, and proposed rescindments for their respective systems of records to the PCLD for review and SAOP approval before they are published. Through the publication of Privacy Act SORNs, the PCLD invites public comments on the activities described in the notice, the proposed sharing of information via routine uses, and any exemptions proposed for the system of records. While public comments to DoW SORNs and associated exemption rules are relatively infrequent, this is an important feedback mechanism available to the public to express concerns on the collection, use, and sharing of individuals' personal information in an agency system of records, and to have those concerns considered and addressed by the DoW PCLO. Table 1 lists the number of SORNs reviewed, approved, forwarded to OMB and Congress, and sent to the Office of the Federal Register for publication during the reporting period.

### **B. Exemption Rule Reviews**

A Privacy Act exemption rule is promulgated when an agency exempts a particular system of records from certain provisions of the Act.<sup>8</sup> The PCLD and the OGC review Privacy Act exemption rules prior to publication in the *Federal Register*. Table 1 lists the number of new and modified exemption rules published as a final rule during the reporting period.

### **C. Matching Agreement Reviews**

A matching agreement is a written agreement between a source agency and a recipient Federal agency or non-Federal agency that specifies the terms by which data from two or more automated systems of records is compared between the agencies, typically to establish or verify the eligibility of individuals for a specific Federal benefit.<sup>9</sup> The PCLD and the OGC review

---

<sup>7</sup> See 5 U.S.C. § 552a(e)(4).

<sup>8</sup> See 5 U.S.C. § 552a(j), (k).

<sup>9</sup> See 5 U.S.C. § 552a(a)(8) and (o).

matching agreements before they are presented for approval to the Data Integrity Board, which was chaired by the ATSW(PCLT). The Chief, PCLD, served as the Executive Secretary for the Data Integrity Board, facilitating the review process for all DoW matching agreements. Table 1 lists the number of matching agreements reviewed and completed during the reporting period, in which DoW is either the source agency or the recipient agency.

#### **D. Privacy Breach Reviews**

A breach is defined as “[t]he loss of control, unauthorized disclosure, unauthorized acquisition or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an unauthorized user accesses PII for other than an authorized purpose.”<sup>10</sup> DoW and OSW Components report privacy breaches impacting DoW personnel to the PCLD, which provided breach reviews, response assistance, as appropriate, and compiled the breach reports to identify and analyze trends. Table 1 lists the number of privacy breaches reported by all DoW and OSW Components and reviewed by PCLD during the reporting period.

#### **E. Social Security Number Justification Reviews**

DoW and OSW Components must submit a Social Security Number (SSN) Justification Memorandum to the PCLD requesting authorization to collect and use SSNs within information systems, forms, and mailings. The justification must comply with Departmental direction establishing limitations on the collection and use of SSNs.<sup>11</sup> Upon receipt, the justification is reviewed, and a decision is made on whether to grant or deny the Component’s request. This effort aims to reduce the use of SSNs, thereby minimizing the risk of SSN misuse or compromise throughout the Department. Table 1 lists the number of SSN Justification Memoranda reviewed and decided on during the reporting period.

#### **F. DoW Issuances, Federal Legislation, Testimonies, and Reports**

The OATSW(PCLT) reviewed DoW-wide issuances for privacy and civil liberties

---

<sup>10</sup> OMB M-17-12, “Preparing for and Responding to a Breach of Personally Identifiable Information,” January 3, 2017.

<sup>11</sup> DoD Instruction 1000.30, “Reduction of Social Security Number (SSN) Use Within DoD,” August 1, 2012, as amended.

equities and provided feedback as appropriate.<sup>12</sup> In addition, the Office reviewed proposed legislation, testimonies, and reports for privacy and civil liberties matters as well as other federal agency documents upon request. Table 1 lists the number of reviews of issuances, legislation, testimonies, and reports conducted during the reporting period.

**Table 1: Privacy and Civil Liberties Reviews from October 1, 2024, to September 30, 2025**

<b>PRIVACY AND CIVIL LIBERTIES REVIEWS</b>	
<b>Type of Review</b>	<b>Number of Reviews</b>
SORNs	
➤ New	5
➤ Modified	6
➤ Rescinded	33
Exemption Rules	1
Matching Agreements <sup>13</sup>	2
Privacy Breach Reviews	2,807
SSN Justification Memoranda	41
DoW Issuances, Federal Legislation, Testimonies, and Reports	407

#### **IV. MATTERS OF ADVICE AND PROGRAMMATIC ACHIEVEMENTS**

The OATSW(PCLT) provided advice on DoW Component privacy and civil liberties matters. This advice served as important guidance for DoW Component Privacy and Civil Liberties Program implementation.

##### **A. Advice**

For the purpose of this Report, advice encompasses the issuance of DoW-wide policies, procedures, or guidance pertaining to privacy and civil liberties. The DoW is actively updating

<sup>12</sup> A DoW issuance establishes or implements DoW policy, designates authority, assigns responsibilities, or provides procedures. Issuances apply to more than one DoW Component. See DoDI 5025.01, “DoD Issuances Program.”

<sup>13</sup> Includes re-establishments of matching agreements; does not include matching agreement renewals of up to one additional year in accordance with 5 U.S.C § 552a(o)(2)(D).

its foundational documents to reflect advances in knowledge, technology, legal developments, and regulatory guidance. Issuances under review and revision during the reporting period include DoDI 5400.11, DoD Privacy and Civil Liberties Programs,” DoD 5400.11-R, “Department of Defense Privacy Program,” and DoDM 5400.11, Volume 2, “DoD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan.”

## **B. Programmatic Achievements**

The following activities highlight key DoW privacy and civil liberties offices’ programmatic efforts during the reporting period:

- The OATSW(PCLT) hosted a Department-wide Privacy Summit as part of Data Privacy Week, convening more than 450 participants to advance collaboration and information-sharing among DoW privacy professionals. The event featured seven guest speakers, and a keynote address focused on the expanding convergence of cyber operations and data privacy, underscoring the need for sustained vigilance in an increasingly interconnected environment.
- The OATSW(PCLT) continued to work to integrate privacy into the Department’s Risk Management Framework (RMF). The OATSW(PCLT) developed and deployed new language on the Department’s Cyber Security Knowledge Service that reflects RMF policy and procedure changes, including updates published by the National Institute of Standards and Technology. Additionally, OATSW(PCLT) expanded its RMF expertise to support Components more effectively in developing policy, sharing knowledge, and responding to RMF inquiries. OATSW(PCLT) also continued to execute its new Privacy RMF training series for DoW privacy officials and system managers. The Privacy RMF training focused on the requisite responsibilities assigned to privacy officials; the steps in the RMF process; key privacy integration points; and the privacy-related controls and evidence used to ensure systems have the appropriate safeguards in place to protect the privacy of individuals. Over the course of several training sessions, an average of about 160 privacy staff were trained using a combination of lectures, exercises, and knowledge checks.

- The OATSW(PCLT) continued its collaboration with the Department’s cross-functional RMF Technical Advisory Group (RMF TAG) to identify mandatory Privacy Enhancing Controls. OATSW(PCLT) also proactively focused on the unique privacy risks posed by artificial intelligence (AI). The OATSW(PCLT) coordinated with the RMF TAG to identify and define a baseline set of privacy-related controls to be applied when an AI application is deployed.
- The OATSW(PCLT) advanced a key initiative to modernize the Department’s privacy governance and align with federal directives on responsible AI use. The Department reviewed its policies and evaluated options for updates to reflect contemporary technological and policy developments. Workgroups across the Department comprised of subject matter experts from privacy, information technology, security, and AI offices remained actively engaged in shaping the Department’s privacy governance framework and charting the path forward.
- The OATSW(PCLT) updated the Department’s privacy compliance documentation to implement E.O. 14168, “Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government,” and E.O. 14249, “Protecting America’s Bank Account Against Fraud, Waste, and Abuse.” As part of this effort, all DoW SORNs were reviewed, and 132 SORNs were identified containing references to the term gender, which have now been replaced to reflect E.O. 14168’s directive. In addition, 18 SORNs were identified for updates to their routine uses sections to align with E.O. 14249 and OMB Memorandum M-25-32, “Preventing Improper Payments and Protecting Privacy Through Do Not Pay.” These actions underscore the Department’s commitment to safeguarding individual privacy, ensuring the accuracy of Federal records, and protecting public resources through strengthened accountability measures.
- The OATSW(PCLT) continued a process of establishing and transitioning to Department-wide SORNs to help standardize the practices concerning the collection, maintenance, use, and sharing of PII in key areas across the enterprise. In furtherance of that effort, the Department published four new Department-wide SORNs and rescinded 33 Component-specific SORNs. Department-wide SORNs aim to reduce duplicative and overlapping SORNs published by separate

Components across the Department. The creation of Department-wide SORNs is expected to make it easier for Department personnel and the public to locate relevant SORNs and create efficiencies in the operation of the Department's privacy program.

- The OATSW(PCLT) supported the development, coordination, and approval of Matching Agreements for the Department's matching programs, resulting in the approval of two 18-Month Re-Establishment Agreements and publication of associated matching notices in the Federal Register and the approval of four One-Year Renewal Agreements to continue operations on six total matching programs. Matching Programs are a critical component of the Department's ability to exchange data with partner agencies and verify eligibility for benefits to include health care, education, compensation, and pension benefits.
- The OATSW(PCLT) launched a Privacy Compliance Support Outreach Program to strengthen governance and accountability across Components. Specifically, PCLD staff partnered with the IOD team and conducted a joint effort compliance visit to two Components to support risk assessment and compliance efforts. This initiative provided targeted risk assessments to identify and mitigate privacy vulnerabilities, while also delivering structured support for the development and refinement of Component level privacy program plans.
- The OATSW(PCLT) advanced a major modernization initiative by deploying electronic solutions that redefined how the Department manages its annual PCLO Report, which was previously a manual process. The OATSW(PCLT) leveraged automation to streamline reporting and strengthen operational efficiencies across the privacy program, transforming compliance into a strategic capability. The new system enabled Components to directly enter and submit data for centralized compilation, while providing real-time metrics and process tracking to enhance oversight and accountability.
- The OATSW(PCLT) established a monthly Department-wide forum to convene Components and subject matter experts for focused discussions on emerging trends, vulnerabilities, and best practices concerning breach prevention and response. This forum serves as a collaborative platform to share lessons learned,

exchange technical insights, and highlight proactive measures that reduce the likelihood of breach occurrences. By fostering regular dialogue and cross-Component engagement, the Department continues its efforts to enhance its ability to anticipate risks, implement effective safeguards, and ensure consistent application of privacy protections across the enterprise.

#### Component-specific Programmatic Achievements:

- In alignment with its mission to safeguard national security through advanced geospatial intelligence, the National Geospatial-Intelligence Agency (NGA) significantly strengthened its Privacy and Civil Liberties Program through enterprise-wide modernization efforts. NGA delivered 17 tailored Role-Based Training modules to more than 1,000 personnel with elevated access to PII, ensuring mission partners across the enterprise possess the knowledge and tools necessary to manage sensitive information responsibly. NGA also advanced the professionalization of its Privacy and Civil Liberties Officer cadre through full-day certification sessions and structured board engagements, enhancing transparency and elevating program maturity. NGA completed substantive updates to its governing policy, formalizing its inspection program, expanding breach response integration, and establishing clear requirements for PII maintained in systems of records. Additionally, NGA embedded privacy considerations into the development and governance of AI initiatives, including AI impact assessments and generative AI guidance. Collectively, these efforts demonstrate NGA's commitment to responsible innovation, workforce readiness, and enterprise-level privacy governance.
- To support its mission of delivering disciplined, modernized, and accountable information governance across the Department of the Army (Army) enterprise, the Army Privacy and Civil Liberties Office implemented several transformative initiatives that strengthened compliance, transparency, and operational efficiency. The Army published comprehensive guidance addressing the intersection of artificial intelligence, records management, FOIA, and privacy, ensuring emerging technologies are deployed responsibly and in accordance with federal

requirements. The Army Records Management Directorate launched a centralized Privacy Impact Assessment (PIA) Portal and public-facing website, providing a unified platform for managing, tracking, and documenting PIAs across the enterprise. This modernization effort enhances consistency, reduces administrative burden, and improves visibility for internal and external stakeholders. The Army also updated its Privacy and Civil Liberties Overview Training to align with recent Executive Orders, and implemented a SORN Reduction Plan that rescinded redundant notices and consolidated overlapping systems. These achievements collectively strengthen the Army's privacy posture, support modernization priorities, and reinforce public trust in the stewardship of personal information.

- In support of its mission to deliver decision-advantage to national security leaders, the Defense Intelligence Agency (DIA) executed a comprehensive transformation of its Privacy and Civil Liberties Program, resulting in a more integrated, efficient, and strategically aligned governance structure. DIA established a Privacy and Civil Liberties Liaison Initiative to embed privacy expertise across organizational units, ensuring consistent application of privacy requirements throughout the agency's operational and analytical environments. The agency strengthened collaboration with the Chief Information Officer's (CIO) RMF team, enabling more precise privacy evaluations for information technology systems and improved alignment with SORN requirements. DIA also revitalized workforce capabilities through targeted training and outreach, enhancing awareness and elevating compliance across the enterprise. Additionally, DIA streamlined its Privacy Act Statement delivery processes, improving service to internal stakeholders while maintaining regulatory rigor. These efforts reflect DIA's commitment to operational excellence, responsible information stewardship, and proactive privacy governance.
- To enhance transparency, accountability, and compliance across the Department of the Navy (DON), the DON CIO Privacy Office implemented a series of enterprise-level improvements to modernize its PIA process. The office successfully launched and enhanced the DON PIA SharePoint Workflow,

providing a standardized, automated routing and approval mechanism that improves visibility at all levels of the organization. This modernization effort ensures PIAs are processed efficiently, consistently, and in accordance with evolving statutory and regulatory requirements. The DON CIO also issued a corresponding policy memorandum establishing clear authority requirements for PIA approval and routing, further strengthening governance and reducing procedural ambiguity. These enhancements not only improved the user experience for submitters but also enabled the closure of a Naval Audit Service finding, demonstrating the DON's commitment to continuous improvement and audit responsiveness. Collectively, these achievements reinforce the Navy's dedication to responsible data stewardship and enterprise-wide compliance.

- Consistent with its oversight mission to promote integrity, accountability, and transparency across the Department, the DoW Office of Inspector General (OIG) advanced several high-impact initiatives that strengthened privacy governance and compliance within the Component. The OIG developed a comprehensive Privacy Dashboard to track SORN and PIA compliance, providing leadership with real-time visibility into program status and enabling data-driven decision-making. The office completed Privacy and Civil Liberties reviews for six instructions and one policy memorandum, ensuring alignment with statutory and regulatory requirements. Additionally, the OIG conducted 10 Privacy Threshold Analyses, which resulted in the rescindment of two outdated SORNs and the creation of compliance documentation for three information collection systems. These achievements demonstrate the OIG's commitment to rigorous oversight, continuous improvement, and the protection of individual privacy rights.

## **V. COMPLAINTS**

Consistent with 42 U.S.C. § 2000ee-1, DoW policy requires DoW Components to have procedures for processing complaints from individuals alleging the DoW violated their privacy

or civil liberties.<sup>14</sup> Generally, the receiving Component Privacy and Civil Liberties Program Office reviews the complaints and reports them to the Component command or other appropriate official. The command will initiate an inquiry and, as necessary, direct corrective action. The complaints counted in this Report, listed in Table 2, were received in accordance with these procedures. For the purpose of this Report, a complaint is an allegation of a violation of an individual's privacy rights, civil liberties, or an alleged violation of conscience, moral principles or religious beliefs in accordance with Section 533 of Public Law 112-239, as described below. Complaints received through Privacy and Civil Liberties Program Offices for which established formal procedural avenues of redress exist, such as complaints alleging a violation of the HIPAA Rules and complaints addressed by the Equal Employment Opportunity or Military Equal Opportunity program offices, are outside the scope of this Report. Similarly, complaints alleging sexual assault or sexual harassment addressed by Department or component sexual assault or harassment prevention and response offices, and certain complaints addressed through the military justice system, such as complaints against alleged perpetrators that result in military courts-martial, are generally reported pursuant to different legal authorities and procedures; therefore, they are also outside the scope of this Report.

As mentioned above, during the reporting period, OATSW(PCLT) launched a new PCLO Reporting Tool to support its ongoing commitment to transparency, streamlined administrative processes, and improved operational efficiency. The tool provided Components with an electronic alternative to the Department Form DD 2984 for submitting inputs to their respective DoW Privacy and Civil Liberties Offices. It also enabled Components to record complaints on a rolling basis throughout the year. Each submission creates a discrete entry, feeding into dynamic dashboards and customized metrics for individual Components, while also allowing OATSW(PCLT) to conduct Department-wide trend analysis and insights.

Additionally, this Report includes civil liberties-related complaints filed by Military Service members or chaplains alleging violations of Section 533 of Public Law 112-239, as amended (Section 533), and DoDI 1300.17, "Religious Liberty in the Military Services," concerning accommodations for individual expressions of conscience, moral principles, or

---

<sup>14</sup> See DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019.

religious beliefs.<sup>15</sup> These Section 533 complaints are reported separately by DoW and OSW Components from other privacy and civil liberties complaints. Service members and chaplains are not required to file Section 533 complaints with the Component privacy and civil liberties program office, but may file them through other offices, such as the Component’s Office of Inspector General. This Report; however, only provides information on the number of Section 533 Complaints received by a Component’s privacy and civil liberties program office. Notably, there were no Section 533 Complaints received during this timeframe.

### **A. Complaint Dispositions**

Table 2 lists the number of privacy and civil liberties complaints received by DoW Components during the reporting period, and the disposition of the complaint. A disposition of “Responsive action taken” means the complaint was reviewed and resolved. It includes any action taken to remediate the violation and prevent recurrence, as well as the determination that the complaint was unsubstantiated. “Pending” indicates the complaint is under review to determine the necessary actions to resolve the complaint. For examples of DoW complaints, please refer to the Appendix of this Report.

### **B. Privacy Complaints**

A privacy complaint is an allegation of a violation of privacy protections in the administration of the programs and operations of the Department. Privacy complaints are separated into five categories in Table 2:

- Process and Procedure Issues (such as appropriate consent, collection, disclosure, and/or notice);
- Redress Issues (non-Privacy Act inquiries seeking resolution of difficulties about privacy matters);

---

<sup>15</sup> Section 533 of Public Law 112-239, as amended, and DoD Instruction 1300.17, “Religious Liberty in the Military Services,” require accommodations of individual expressions of beliefs of members of the armed forces that reflect their sincerely held conscience, moral principles, or religious beliefs unless such accommodations would have an adverse impact on military readiness, unit cohesion, and good order and discipline; such expression of accommodations may not, in so far as practicable, be the basis of an adverse personnel action, discrimination, or denial of promotion, schooling, training, or assignment. These authorities also prohibit requiring chaplains to perform rites, rituals, or ceremonies contrary to their conscience, moral principles, or religious beliefs and prohibit discrimination or adverse actions against chaplains on such a basis.

- Operational Issues (such as issues of day-to-day operations);
- Referred to Other Agency; and
- Other.

### **C. Civil Liberties Complaints**

A civil liberties complaint is an allegation of a violation of civil liberties in the administration of the Department's programs and operations. For the purpose of this Report, civil liberties complaints involve the assertion of a violation of the rights and freedoms guaranteed by the first 10 amendments to the U.S. Constitution (i.e., the Bill of Rights). The types of civil liberties complaints reported may include, but are not limited to:

- First Amendment (e.g. freedom of speech, religion, press, right to assemble peaceably, and right to petition for redress of grievances);
- Second Amendment (right to keep and bear arms);
- Fourth Amendment (protection against unreasonable search and seizure);
- Fifth Amendment (protection against double jeopardy and self-incrimination, right to due process (including equal protection));
- Sixth Amendment (right to speedy and public trial/counsel/calling of witnesses/confronting of accusers);
- Eighth Amendment (protection against cruel/unusual punishments/excessive fines/bail); and
- Ninth Amendment (unremunerated rights).

### **D. Complaints Alleging Violations of Conscience, Moral Principles or Religious Beliefs Under Section 533 of Pub. Law 112-239, as amended**

This subsection will only apply to complaints by Military Service members, including chaplains, premised on Section 533 of Pub. Law 112-239, as amended. Section 533, as amended by Section 532 of Public Law 113-66, provides certain protections for the rights of conscience, moral principles, and religious beliefs of members of the Armed Forces and Chaplains as follows:

- Unless it could have an adverse impact on military readiness, unit cohesion, and

good order and discipline, the Armed Forces shall accommodate individual expressions of belief of a member of the armed forces reflecting the sincerely held conscience, moral principles, or religious beliefs of the member and, in so far as practicable, may not use such expression of belief as the basis of any adverse personnel action, discrimination, or denial of promotion, schooling, training, or assignment.

- No member of the Armed Forces may require a chaplain to perform any rite, ritual, or ceremony that is contrary to the conscience, moral principles, or religious beliefs of the chaplain; or discriminate or take any adverse personnel action against a chaplain, including denial of promotion, schooling, training, or assignment, on the basis of the refusal by the chaplain to comply with such a requirement.

**Table 2: Privacy and Civil Liberties Complaints  
(received via Privacy and Civil Liberties Program Offices)**

Nature of Privacy Complaints	Number Received	Disposition of Complaint	
		Responsive Action Taken	Pending
Process and Procedure	75	65	10
Redress Issues	0	0	0
Referred to Other Agency	2	2	0
Operational Issues	1	1	0
Other	1	1	0
<b><i>Sub Total for Privacy Complaints:</i></b>	<b>79</b>	<b>69</b>	<b>10</b>
Nature of Civil Liberties Complaints	Number Received	Responsive Action Taken	Pending
First Amendment	2	2	0
Fourth Amendment	2	2	0
Fifth Amendment	9	9	0
<b><i>Sub Total for Civil Liberties Complaints:</i></b>	<b>13</b>	<b>13</b>	<b>0</b>
Complaints Alleging Violations of Conscience, Moral Principles or Religious Beliefs Under Section 533 of Pub. Law 112-239, as amended	Number Received	Responsive Action Taken	Pending
Complaints by Military Service Members	0	0	0
Complaints by Chaplains	0	0	0
<b><i>Sub Total for Section 533 Complaints</i></b>	<b>0</b>	<b>0</b>	<b>0</b>
<b>TOTAL COMPLAINTS FY 2025</b>	<b>92</b>	<b>82</b>	<b>10</b>

## **CONCLUSION**

In accordance with Section 803, this Report summarizes the activities of the DoW PCLO from October 1, 2024, through September 30, 2025. The DoW will continue to work with Congress, the OMB, the PCLOB, and other federal agencies to ensure it appropriately protects privacy and civil liberties. Program activities and accomplishments serve to assure the continuing protection of privacy and civil liberties in each of the functions and missions of the Department.

## APPENDIX: Samples of Privacy and Civil Liberties Complaints

### Sample DoW Privacy Complaints<sup>16</sup>

#### *Sample Complaint #1:*

**Description of Complaint:** Complainant alleged that personal information was improperly disseminated, resulting in unauthorized individuals receiving access to protected data.

**Findings:** Substantiated. An inquiry confirmed that personally identifiable information was improperly shared. Corrective measures were implemented to prevent recurrence.

**Disposition:** Responsive Action Taken.

#### *Sample Complaint #2:*

**Description of Complaint:** Complainant alleged that an individual improperly obtained their personally identifiable information, without consent, with the intent to use it for personal reasons.

**Findings:** Un-substantiated. Investigation determined no violations occurred.

**Disposition:** Responsive Action Taken.

### Sample DoW Civil Liberties Complaints

#### *Sample Complaint #1:*

**Nature of Complaint:** First Amendment – Freedom of Speech.

**Description of Complaint:** Complainant alleged that personnel were directed to remove lanyards expressing organizational initiatives, which they believed infringed on protected expression.

**Findings:** Substantiated. Responsive actions were taken, including recalling the directive and issuing formal guidance to clarify permissible expression.

**Disposition:** Responsive Action Taken.

#### *Sample Complaint #2:*

**Nature of Complaint:** Fifth Amendment – Right to Due Process.

**Description of Complaint:** Complainant alleged that a financial recovery action was initiated without proper notice or an opportunity to establish a payment plan.

---

<sup>16</sup> These samples reflect submissions during the reporting period and have been edited to ensure the privacy of the complainant.

**Findings:** Unsubstantiated. The chain of command assisted the complainant in establishing a payment plan to mitigate hardship. No due process violation was found.

**Disposition:** Responsive Action Taken.