

Department of Defense
Privacy and Civil Liberties Officer Report



Semiannual Report for Fiscal Year 2017

April 1, 2017 – September 30, 2017

TABLE OF CONTENTS

I. INTRODUCTION	3
II. THE DOD PRIVACY AND CIVIL LIBERTIES PROGRAM	3
A. The Office of the Deputy Chief Management Officer (ODCMO)	5
B. The Directorate for Oversight and Compliance (DO&C)	5
C. The Intelligence Oversight Division	5
D. The Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD)	5
E. DoD Office of General Counsel (OGC)	6
F. DoD Component Privacy and Civil Liberties Officials	6
1. Senior Component Officials for Privacy (SCOPs) and Component Privacy Officers	6
2. Component Chief Civil Liberties Officers (CCLOs) and Points of Contact (POCs)	6
III. REVIEWS	7
A. System of Records Notice (SORN) Reviews	7
B. Exemption Rule Reviews	7
C. Matching Agreement Reviews	7
D. Privacy Breach Reviews	7
E. Social Security Number Justification Reviews	8
Table 1: Privacy and Civil Liberties Reviews	8
IV. MATTERS OF ADVICE AND RESPONSE	9
A. Advice	9
B. Programmatic Achievements	9
V. COMPLAINTS	9
Table 2: Privacy and Civil Liberties Complaints	11
VI. CONCLUSION	11
APPENDIX: Samples of Privacy and Civil Liberties Complaints	i
Sample DoD Privacy Complaints	i
Sample DoD Civil Liberties Complaints	i

I. INTRODUCTION

The Department of Defense (“DoD” or “Department”) submits this Privacy and Civil Liberties Officer Report covering the activities of the DoD Privacy and Civil Liberties Officer (PCLO) for the second semiannual reporting period of fiscal year 2017: April 1, 2017 through September 30, 2017.

Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110-53), 42 U.S.C. § 2000ee-1 (hereinafter referred to as “Section 803”) requires the DoD to designate a senior officer to serve as the Department’s principal advisor on privacy and civil liberties matters, and to report on a semiannual basis the activities of this officer.¹ The Deputy Chief Management Officer (DCMO)² of the Department serves as the PCLO and reports to and advises the Deputy Secretary of Defense and the Secretary of Defense on these matters.

Section 803 Reports describe the privacy and civil liberties activities of the DoD PCLO, including:

- Information on the number and types of reviews undertaken;
- The type of advice provided and the response given to such advice;
- The number and nature of the privacy and civil liberties complaints received by the Department; and
- A summary of the disposition of such reported complaints, the reviews and inquiries conducted, and the impact of the activities of such officer.

The DoD 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 dedication to leadership and collaboration in this area, this report includes the activities of the PCLO in establishing policy and guidelines, the efforts of other DoD privacy and civil liberties officials who implement those policies, and the compliance mechanisms which safeguard the personal information, privacy, and civil liberties of individuals.³

II. THE DOD PRIVACY AND CIVIL LIBERTIES PROGRAM

The DoD Privacy and Civil Liberties Program was established to ensure compliance with the federal statutes governing privacy and civil liberties, as well as the Office of Management and Budget (OMB) guidelines. On behalf of the PCLO, the Directorate for Oversight and Compliance (DO&C) effects DoD policy, and directs and oversees compliance of the DoD component privacy and civil liberties programs.

The DoD Privacy and Civil Liberties Program began with the establishment of the Defense Privacy Office in 1975, after the passage of Section 552a of Title 5, United States Code (U.S.C.), also known as “The Privacy Act of 1974.”⁴ When the Implementing Recommendations of the 9/11 Commission Act of 2007, Section 803 was enacted, the Department expanded the mission of the

¹ See 42 U.S.C. § 2000ee-1, “Implementing Recommendations of the 9/11 Commission Act of 2007.”

² See <http://dcmo.defense.gov/Home.aspx> for further information regarding the Office of the Deputy Chief Management Officer.

³ As defined in 5 U.S.C. 552a.(a)(2).

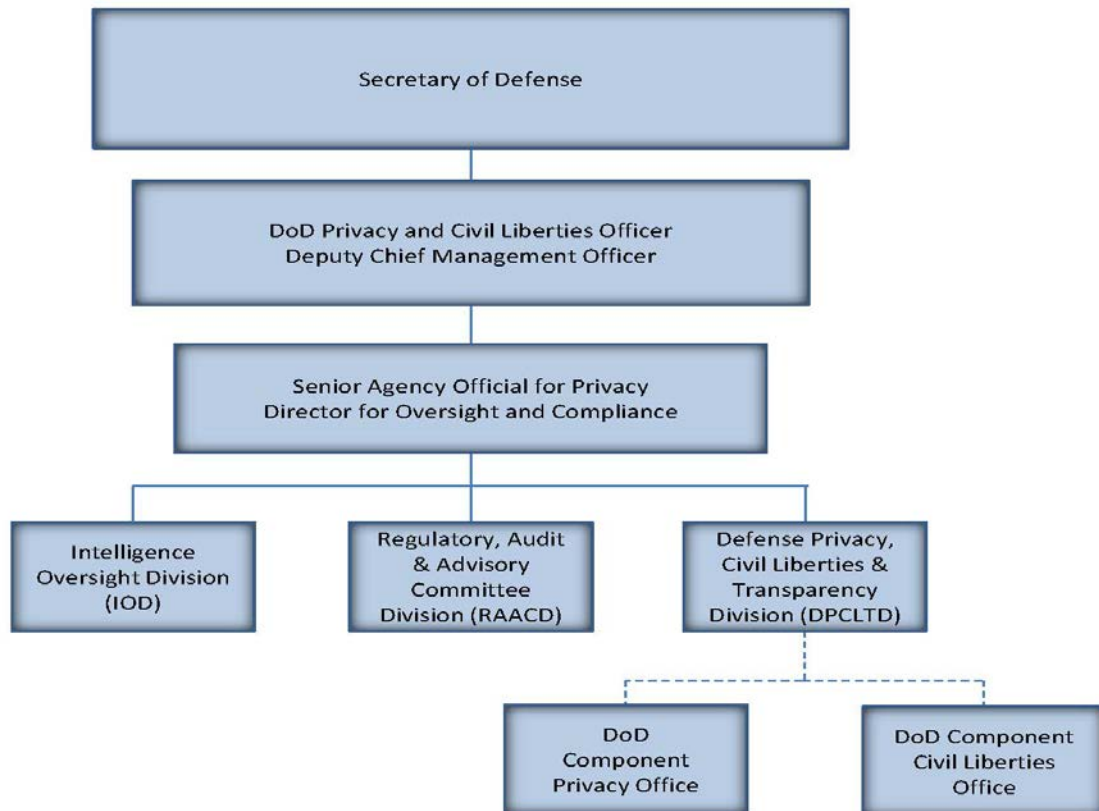
⁴ The Privacy Act of 1974, 5 U.S.C. § 552a (2012) took effect on September 27, 1975, and can generally be characterized as an omnibus “code of fair information practices” that attempts to regulate the collection, maintenance, use, and dissemination of personal information of individual by federal executive branch agencies.

Defense Privacy Office and renamed it as the Defense Privacy and Civil Liberties Office. As capabilities in information technology and information management have become increasingly sophisticated and diverse, the DoD privacy and civil liberties programs ensure the ongoing protection of individual rights, consistent with the missions of the Department. The DoD privacy and civil liberties policies and procedural requirements are established in DoD Directive (DoDD) 5400.11, “DoD Privacy Program,” October 29, 2014;⁵ DoD 5400.11-R, “Department of Defense Privacy Program,” May 14, 2007;⁶ and DoD Instruction (DoDI) 1000.29, “DoD Civil Liberties Program,” December 14, 2014.⁷

As a result of changes in guidance by the OMB from July 2016 through September 2017, the DoD issuances cited above are being revised. In addition, as part of the review of the Department’s federal regulations, the DoD privacy regulation (32 C.F.R. Part 310) is being rewritten as a single DoD wide rule, and will result in the rescission of 20 separate DoD Component regulations to promote uniformity across the Department.

Because of its size and the diversity of its functions, the Department employs a decentralized structure for implementing its privacy and civil liberties programs. This approach enables the DoD to comply with federal agency requirements and ensure that privacy and civil liberties are appropriately considered in all Department activities. Figure 1 provides the structure and responsibilities of the DoD Privacy and Civil Liberties Program.

Figure 1: DoD Privacy and Civil Liberties Program Structure



⁵ Available at <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/540011p.pdf>

⁶ Available at <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/540011r.pdf>

⁷ Available at <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/100029p.pdf>

A. The Office of the Deputy Chief Management Officer (ODCMO)

The Deputy Chief Management Officer (DCMO) serves as the DoD PCLO and reports to and advises the Deputy Secretary of Defense, who is the Chief Management Officer, and the Secretary of Defense. Other DCMO responsibilities include advising the Secretary and Deputy Secretary on business transformation, and leading the Department's efforts to streamline business processes and improve efficiencies in headquarters structure. The DCMO serves to coordinate the business operations of the Department and, in a broad capacity, exercises oversight authority throughout the Department. As the PCLO, the DCMO is responsible for ensuring that the privacy and civil liberties of individuals are appropriately protected.

B. The Directorate for Oversight and Compliance (DO&C)

The DO&C within the ODCMO comprises three divisions: the Intelligence Oversight Division (IOD), the Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD), and the Regulatory and Advisory Committee Division. The Director of O&C reports to the DCMO and is charged with implementing the Department's privacy and civil liberties programs. This includes ensuring compliance with the Privacy Act, as well as ensuring processes are in place to protect the privacy and civil liberties of individuals in accordance with the law. This includes implementation of agency guidance and oversight on privacy and civil liberties from the OMB and the Chief Executive's Privacy and Civil Liberties Oversight Board.

The Director of O&C has also been designated as the DoD Senior Agency Official for Privacy (SAOP). The SAOP has Department-wide responsibility for privacy, including protection of personal information of individuals, compliance with Federal laws, regulations, and policies, and influencing legislative, regulatory, and other policy initiatives that implicate Privacy Act compliance and information risk management. The SAOP establishes the parameters of DoD Privacy and Civil Liberties Program for the Department. The SAOP relies on the Intelligence Oversight Division (IOD) and interfaces with intelligence colleagues to ensure that matters sensitive to national security are scrutinized appropriately. Finally, the SAOP routinely provides information and recommendations directly to the PCLO.

C. The Intelligence Oversight Division (IOD)

The IOD is responsible to the Secretary of Defense for the independent oversight of all intelligence, counterintelligence, and intelligence-related activities of the Department. The IOD inspects all intelligence or intelligence-related activities conducted by any of the DoD Components to ensure that these activities comply with federal law, Executive Orders, Presidential Directives, Intelligence Community Directives, and DoD issuances. Due to the importance of protecting privacy and civil liberties when conducting intelligence activities, the IOD is an integral part of the DoD Privacy and Civil Liberties Programs. The Chief, IOD also serves as the DoD Senior Intelligence Oversight Official (SIOO), reporting directly to the Secretary of Defense, and serves as the Deputy Director, DO&C.

D. The Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD)

As a division of the Oversight and Compliance Directorate, the DPCLTD assists the PCLO and DO&C/SAOP in implementing the DoD Privacy and Civil Liberties Program by providing guidance to Component officials, reviewing publications and legislative activities, facilitating official reporting, and providing training in both privacy and civil liberties content and program administration.

The DPCLTD communicates routinely on a wide range of activities with privacy and civil liberties officials at each DoD Component, the OMB, the Privacy and Civil Liberties Oversight Board (PCLOB), and other Federal departments and agencies, to facilitate the Department-wide execution of Federal privacy and civil liberties program requirements, and to exchange ideas on the development and business practices for privacy and civil liberties.

E. The DoD Office of General Counsel (OGC)

The DoD OGC provides legal advice to the DO&C, the DPCLTD, and other DoD officials, also augmenting the legal advisors of the DoD Components directly in support of the DoD privacy and civil liberties program. In addition to the many attorneys throughout the Department who work on privacy and civil liberties matters, including complaints, the DoD OGC has assigned legal advisors to work directly with the DO&C and the DPCLTD to provide legal reviews for privacy and civil liberties issues and to ensure that the development of privacy and civil liberties policy is consistent with the law.

F. DoD Component Privacy and Civil Liberties Officials

The DoD Components – including each Military Department and the various Defense agencies -- are responsible for administering privacy and civil liberties programs, including the establishment and implementation of Component-level privacy and civil liberties policies, procedures, and training coincident with DoD issuances and guidelines. The Director of O&C and the Chief, DPCLTD communicate regularly with privacy and civil liberties officials in their respective capacities within DoD Components to ensure compliance with law and policy.

1. Senior Component Officials for Privacy (SCOPs) and Component Privacy Officers (CPOs)

Recognizing the large, decentralized nature of the Department, to ensure that privacy remains a focus throughout the Department, the SAOP requires the head of each DoD Component to designate a SCOP. Each SCOP must be a general/flag officer or member of the Senior Executive Service and oversees existing or potential compliance issues requiring executive level intervention, and to identifies the issues and recommends action for matters needing the attention of the appropriate Component leadership. In addition, the SCOPs provide information and policy advice to the Director, DO&C/SAOP to assist in decision-making at the Departmental level.

DoD CPOs and support staff assist the SCOPs at the Service, Component, and Combatant Command levels. They perform the day-to-day privacy functions, collect data, and respond to inquiries and complaints of alleged violations of the Privacy Act along with ensuring documentation of compliance throughout their respective organizations.

2. Component Chief Civil Liberties Officers (CCLOs) and Points of Contact (POCs)

DoD Components are also responsible for designating a senior service member or civilian employee to serve as the CCLO, and another service member or civilian employee to serve as the Component's civil liberties POC. Generally, the CCLO has authority to act on behalf of the Component Head to direct the Component's compliance with Section 803 and the DoD Civil Liberties Program. The civil liberties POC is responsible for fulfilling the day-to-day and reporting requirements of the DoD Civil Liberties Program within the Component, under the direction of the CCLO.

III. REVIEWS

The DoD considers privacy and civil liberties concerns when proposing, developing, and implementing laws, regulations, policies, procedures, and guidelines.⁸ On behalf of the DCMO and the Director of O&C, the DPCLTD reviews all Department-level issuances, as well as proposed federal legislation, testimony, and reports for impacts on privacy and civil liberties, recommending changes when appropriate. When requested, the DPCLTD reviews and comments on other federal agency documents which may affect the Department's operations. The total number of documents reviewed by the DPCLTD during this review period is identified in Table 1.

Privacy and civil liberties reviews are conducted in accordance with guidance generally established by the OMB and in consultation with the DoD OGC. The Department also ensures compliance and alignment with the Federal Information Security Modernization Act of 2014 and the E-Government Act of 2002 (44 U.S.C. § 3501) with respect to information management requirements. For the purposes of this report, privacy compliance reviews are enumerated as follows and are summarized in Table 1:

A. System of Records Notice (SORN) Reviews

A SORN is a notice published by an agency in the *Federal Register* upon the establishment or modification of a system of records, describing the existence and character of that system.⁹ DoD Components must submit their SORNs for their respective systems of records to DPCLTD for review, and agency approval. Table 1 lists the number of SORNs that DPCLTD has reviewed, approved, forwarded to OMB and Congress, and sent to the Office of the Federal Register for publication during this review period.

B. Exemption Rule Reviews

A Privacy Act exemption rule is promulgated when a system of records is exempted from certain general or specific provisions of the Privacy Act of 1974, as amended.¹⁰ For the purposes of this report, the number of exemption rules reported in Table 1 represents new exemption rules reviewed by DPCLTD and the DoD OGC and published as a final rule during the reporting period.

C. Matching Agreement Reviews

Matching Agreement (MA) Reviews – An MA is a written agreement between a source agency and a recipient agency (federal or non-federal agency) when automated systems of records data is matched between the agencies, typically to determine the eligibility of individuals for a specific federal service or benefit.¹¹ For the purposes of this report, the number of MAs reported in Table 1 represents MAs reviewed and completed during this period, in which DoD is either the source agency or the recipient agency.

D. Privacy Breach Reviews

A breach is defined as the 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 or (2) an unauthorized user

⁸ See 42 U.S.C. § 2000ee-1.

⁹ See 5 U.S.C. § 552a (e) (4).

¹⁰ See 5 U.S.C. § 552a (j), (k).

¹¹ See 5 U.S.C. § 552a (8) and (o).

accesses personally identifiable information for an other than authorized purpose.¹² DoD Components are required to report all privacy breaches to the DPCLTD, which compiles the breach reports to identify and analyze trends, and to inform the Department’s senior leadership. The number reported in Table 1 is the total number of privacy breaches across all Components that were reported to DPCLTD during this period.

During the reporting period, the Department of Defense established a Breach Response Plan which incorporates the requirements of OMB Memorandum 17-12, “Preparing for and Responding to a Breach of Personally Identifiable Information,” as well as departmental policy and procedures. This plan will also be incorporated as part of the publication of a DoD Manual 5400.11 which will provide internal guidance for carrying out the Department’s privacy program.

E. Social Security Number (SSN) Justification Reviews

In implementing the Department’s plan to reduce the use of SSNs, DoD policy¹³ requires DoD Components to request approval from DPCLTD for any use of social security numbers in information systems or DoD forms. This effort is intended to reduce and eliminate, where possible, the use of SSNs in DoD information collections. The number reported in Table 1 is the total number of SSN justification memoranda approved by DPCLTD during the reporting period.

Table 1 lists the total number of reviews of the documents mentioned above.

Table 1: Privacy and Civil Liberties Reviews

PRIVACY and CIVIL LIBERTIES REVIEWS	
Type of Review	Number of Reviews
System of Records Notices (SORNs)	
➤ Modifications:	2
➤ Amendments:	3
➤ Rescindments:	0
Exemption Rules	0
Matching Agreements	2
Privacy Breach Reviews	357
SSN Justification Memoranda	9
DoD Issuances, Federal Legislation, Testimony, and Reports:	161

IV. MATTERS OF ADVICE AND RESPONSE

The Office of the DCMO provides advice and documents responses to advice on privacy and civil liberties matters for all DoD Components. This advice and response to advice serves as

¹² OMB M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," January 3, 2017.

¹³ DoDI 1000.30, "Reduction of Social Security Number (SSN) Use Within DoD," August 1, 2012.

important guidance for DoD Component privacy and civil liberties program implementation.

A. Advice

For the purpose of this report, advice encompasses the written issuance of DoD policies, procedures, or guidance pertaining to privacy and civil liberties by the PCLO or SAOP. This includes the SAOP's issuance of formal privacy guidance in its Breach Response Plan, approved in September 2017.

B. Programmatic Achievements

The following activities highlight key DO&C and DPCLTD programmatic efforts during this period:

- The DPCLTD continued its work with the Office of the Chief Information Officer to expand the application of privacy controls to all information systems which contain Personally Identifiable Information and not limited to those systems of records defined in the Privacy Act. The privacy overlays outlined in Committee on National Security Systems Instruction (CNSSI) No. 1253¹⁴ have been designed for this broader approach to protecting personal information.
- DoD privacy subject matter experts provided recommendations for the revision of DoD Instruction 5400.16, "Privacy Impact Assessments," which provides guidance on completing and documenting Privacy Impact Assessments on agency information systems. In addition, DoD privacy subject matter experts provided the CIO staff with recommendations on updating the Department's privacy impact assessments – the first revision in nearly a decade.
- The Risk Management Framework (RMF) also supports the management of privacy information. The RMF Knowledge Service (KS) portal defines privacy categorization and corresponding controls throughout the process of bringing new information systems online.
- The Privacy team conducted training Joint Base Pearl Harbor-Hickam and McGhee Tyson Air National Guard Base and delivered state-of-the-art instruction for over 275 personnel supporting DoD's privacy program stationed in various parts of the world.
- The SAOP received the designations of Senior Component Officials for Privacy (SCOPs), to include representatives from the DoD principal staffs. Establishing SCOPs at the highest levels in the DoD staff and Components provides the SAOP with a wide range of advice and exposure to the Department's myriad programs concerning privacy.
- The Intelligence Oversight Division continues to conduct detailed on-site inspections, and inspection items include ensuring that privacy and civil liberties are respected in the Department's intelligence program.

V. COMPLAINTS

DoD Components are required to have established procedures for processing complaints from individuals who allege violations of their privacy or civil liberties.¹⁵ Complaints received directly by DPCLTD are forwarded to the appropriate DoD Component for further review. Generally, complaints are reviewed by the receiving Component privacy and civil liberties program office and reported to the Component command or appropriate official. Upon receipt of the complaint, the command may initiate an investigation and, as necessary, direct corrective action. The complaints

¹⁴ Attachment 6 to Appendix F, CNSSI No. 1253, Version 2, 15 March 2012.

¹⁵ See DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007; DoDI 1000.29, "DoD Civil Liberties Program," December 14, 2014.

identified in this report at Table 2 were received in accordance with these procedures. For the purposes of this report, a complaint is an allegation of a violation of an individual's privacy rights or civil liberties. Privacy or civil liberties complaints arising out of non-judicial punishments, military courts-martial, and administrative separations are not included in this report. Complaints submitted under the Health Insurance Portability and Accountability Act (HIPAA) are also not listed herein.

This report includes the number of complaints received by DoD Components during the reporting period for which (1) responsive action was taken, or (2) action is pending. "Responsive action taken" means the complaint was reviewed and resolved. It also includes any action taken to remediate the violation and prevent recurrence. "Pending" indicates the complaint is under review to determine what actions may be required to resolve the complaint.

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 three categories:

- Procedural Issues (such as complaints regarding appropriate consent, collection, and/or notice with personally identifiable information);
- Redress Issues (non-Privacy Act inquiries seeking resolution of difficulties about privacy matters); and
- Operational Issues (Privacy Act matters not including requests for access, disclosure, or amendment).

For samples of DoD Privacy Complaints, please refer to the Appendix of this report.¹⁶

A civil liberties complaint is an allegation of a violation of civil liberties in the administration of the programs and operations of the Department. For 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, the Bill of Rights and the Fourteenth Amendment. Types of civil liberties complaints include, but are not limited to:

- First Amendment (e.g. freedom of speech, religion, assembly, and association);
- Second Amendment (right to keep and bear arms);
- Fourth Amendment (protection against unreasonable search and seizure);
- Fifth Amendment (due process);
- Sixth Amendment (speedy and fair trial);
- Eighth Amendment (no cruel/unusual punishment)
- Ninth Amendment ("unenumerated" rights) and
- Fourteenth Amendment ("equal protection").

Examples of DoD civil liberties complaints, provided for illustrative purposes, are also included in the Appendix of this report.

¹⁶ These samples are not actual incidents.

Table 2: Privacy and Civil Liberties Complaints

Nature of Privacy Complaints	Number Received	Disposition of Complaint	
		Responsive Action Taken	Pending
Procedural	4	3	1
Redress	2	2	0
Operational	0	0	0
<i>Sub Total for Privacy Complaints:</i>	6	5	1
Nature of Civil Liberties Complaints			
First Amendment	1	1	0
Second Amendment	0	0	0
Fourth Amendment	12	10	2
Fifth Amendment	48	29	19
Fifth and Fourteenth Amendments	1	1	0
Sixth Amendment	0	0	0
Eighth Amendment	0	0	0
Ninth Amendment	1	0	1
Fourteenth Amendment	1	1	0
<i>Sub Total for Civil Liberties Complaints:</i>	64	42	22
TOTAL 3rd & 4th Qtrs. FY17	70	47	23

VI. CONCLUSION

In accordance with Section 803, this report summarizes the semiannual activities of the DoD Privacy and Civil Liberties Officer from April 1, 2017 through September 30, 2017. DoD will continue to work with Congress, the OMB, the PCLOB, and other federal agencies to ensure that it proactively protects privacy and civil liberties.

APPENDIX: Samples of Privacy and Civil Liberties Complaints¹⁷

Sample DoD Privacy Complaints

Sample Complaint #1:

Description of Complaint: A complainant alleged that a co-worker released PII and other sensitive information about complainant to personnel who did not have a need-to-know.

Findings: Unsubstantiated. It was confirmed that the co-worker did have a need-to-know of the PII. There was no substantial evidence that the PII and other sensitive information was released or shared with other personnel in the office. The complainant was notified. Privacy Act training was conducted to ensure everyone within the directorate understood how to properly handle PII and sensitive information.

Disposition: Responsive Action Taken.

Sample Complaint #2:

Description of Complaint: A complainant alleged that an application form that was used for applying for access was not compliant with the Privacy Act.

Findings: After review of the form, it was found that a Privacy Act statement was required. The information on the form is “For Official Use Only/Freedom of Information Act” (FOUO/FOIA) exempt information and contained PII. The form should be encrypted when sent electronically and safeguarded when stored with limited access by those with a need-to-know, and then destroyed (shredded). In accordance with the reviewing officer’s findings and recommendations, the form in question was revised to make it compliant with the Privacy Act.

Disposition: Responsive Action Taken.

Sample DoD Civil Liberties Complaints

Sample Complaint #1:

Description of Complaint: Alleged Second Amendment violation. The complainant, a soldier, alleged that his unit commander unlawfully confiscated his personally owned weapons.

Findings: Inquiry indicated that the unit had improperly confiscated these weapons. The unit’s confiscation rationale, that the complainant was suspended from duty and under investigation for an inappropriate relationship, was not justified under Section 1062 of the National Defense Authorization Act of FY 2011 and Army policy. The unit returned the personally owned weapons to the soldier.

Disposition: Responsive Action Taken.

Sample Complaint #2:

Description of Complaint: Alleged Fourth Amendment violation. The complainant, a civilian, alleged that security forces violated the complainant’s rights against unlawful search and seizure.

Findings: An internal investigation was conducted and appropriate training was provided.

Disposition: Responsive Action Taken.

¹⁷ These are not actual incidents during the reporting period.