DoD Instruction 5400.11

DoD Privacy and Civil Liberties Programs

Originating Component:	Office of the Chief Management Officer of the Department of Defense
Effective:	January 29, 2019
Releasability:	Cleared for public release. Available on the DoD Issuances Website at http://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014
Incorporates and Cancels:	DoD Instruction 1000.29, "DoD Civil Liberties Program," May 17, 2012, as amended
Approved by:	Lisa W. Hershman, Acting Chief Management Officer of the Department of Defense

Purpose: In accordance with DoD Directives (DoDDs) 5105.53 and 5105.82 and the guidance in the July 11, 2014 Deputy Secretary of Defense Memorandum and the February 1, 2018 Secretary of Defense Memorandum, this issuance:

- Establishes policy, assigns responsibilities, and prescribes procedures for administering the DoD Privacy and Civil Liberties Programs.
- Establishes the Defense Data Integrity Board.

TABLE OF CONTENTS

TABLE

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This issuance applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff, and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense (OIG DoD), the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD, including the DoD Intelligence Components (referred to collectively in this issuance as the "DoD Components").

1.2. POLICY.

a. All DoD Components will:

(1) Establish and maintain comprehensive privacy and civil liberties programs that comply with applicable statutory, regulatory, and policy requirements, and develop and evaluate privacy and civil liberties policies and manage privacy risks.

(2) Comply with all applicable:

(a) Privacy and civil liberties related laws, regulations, and policies, including the requirements of the Privacy Act of 1974, and ensure that Privacy Act system of records notices (SORNs) are published, revised, and rescinded, as required.

(b) Executive orders, Intelligence Community directives, and other applicable guidance to DoD Components conducting intelligence activities with respect to privacy and civil liberties matters (e.g., Executive Order 12333 and DoD Manual 5240.01).

(3) Limit the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of personally identifiable information (PII) maintained in a system of records to that which is legally authorized, relevant, and reasonably deemed necessary to accomplish a DoD function.

(4) Maintain all records with PII in accordance with applicable records retention or disposition schedules approved by the National Archives and Records Administration.

(5) Impose conditions, where appropriate, when sharing PII with other federal and non-federal agencies or entities (including the selection and implementation of particular security and privacy controls) that govern the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of the PII. This will be accomplished using written agreements, including contracts, data use agreements, information exchange agreements, and memoranda of understanding when appropriate.

(6) Maintain adequate procedures to receive, investigate, respond to, and redress complaints from individuals who allege that the DoD has violated their privacy or civil liberties.

(7) In accordance with Section 2000ee-1 of Title 42, U.S.C., prohibit reprisals or threats of reprisal against individuals who make complaints to DoD privacy and civil liberties program

officials or the Privacy and Civil Liberties Oversight Board indicating a possible violation of privacy protections or civil liberties in the administration of Federal Government programs relating to efforts to protect the Nation from terrorism, unless the complaint was made or the information was disclosed with the knowledge that it was false or with willful disregard for its truth or falsity.

b. This issuance does not create any rights, privileges, or benefits, substantive or procedural, enforceable by any party against the United States, its departments, agencies, other entities, its officers, or any other persons.

1.3. INFORMATION COLLECTIONS.

a. The report referenced in Paragraph 2.2.d. of this issuance (required by Chapter 35, Subchapter II, of Title 44, U.S.C., also known and referred to in this issuance as the "Federal Information Security Modernization Act (FISMA)") has been assigned report control symbol DD-CIO(A,Q)2296 in accordance with the procedures in Volume 1 of DoD Manual 8910.01. The expiration date of this information collection is listed in the DoD Information Collections System at https://apps.sp.pentagon.mil/sites/dodiic/Pages/default.aspx.

b. Additional information on the DoD Privacy and Civil Liberties reporting requirements are outlined in DoD 5400.11-R and DoD Instruction (DoDI) 1000.30 respectively.

c. The semi-annual DoD Privacy and Civil Liberties Officer (PCLO) (Section 803) Report is prescribed in Section 2000ee-1 of Title 42, U.S.C.

d. Other reports directed by the OMB and by DoD through the Chief, Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD) have been assigned report control symbol DD-DCMO(Q)2472 in accordance with the procedures in DoDI 5545.02.

SECTION 2: RESPONSIBILITIES

2.1. CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF DEFENSE (CMO). In addition to the responsibilities in Paragraph 2.7., the CMO:

a. Serves as the DoD PCLO in accordance with Sections 2000ee-1 and 2000ee-2 of Title 42, U.S.C.

b. Advises the Secretary of Defense and senior DoD leadership on the DoD Privacy and Civil Liberties Programs.

c. Assists the Secretary of Defense and senior DoD leadership in considering privacy and civil liberties concerns when they propose, develop, or implement laws, regulations, policies, procedures, DoD issuances, or guidelines.

d. When providing advice on proposals to create, retain, or enhance a particular DoD function, considers and determines whether the DoD has established that:

(1) The need for that function is balanced with the need to protect privacy and civil liberties.

(2) There is adequate supervision over that function to ensure protection of privacy and civil liberties.

(3) There are adequate guidelines and oversight to properly confine the extent of the function.

e. Ensures that DoD operations, policies, procedures, guidelines, and issuances and their implementation are periodically investigated, reviewed, and amended to provide for adequate protection of privacy and civil liberties.

f. Designates a Senior Agency Official for Privacy (SAOP) who has DoD-wide responsibility and accountability for developing, implementing, and maintaining a DoD-wide privacy program.

g. Submits semiannual reports on the activities of the DoD Privacy and Civil Liberties Programs to the appropriate congressional committees, the Privacy and Civil Liberties Oversight Board, and the Secretary of Defense, in accordance with Section 2000ee-1 of Title 42, U.S.C. These reports will be available to the public to the greatest extent that is consistent with the protection of classified information and applicable law. (Note: The National Security Agency reports directly to Congress with notification to DoD.)

2.2. DIRECTOR, DIRECTORATE FOR OVERSIGHT AND COMPLIANCE (DO&C). Under the authority, direction, and control of the CMO, the Director, DO&C:

a. Serves as the DoD's SAOP. In accordance with OMB Memorandum M-16-24, OMB Circulars No. A-130 and No. A-108, and Sections 2000ee-1 and 2000ee-2 of Title 42, U.S.C., these duties include:

(1) Taking a central policy-making role in developing and evaluating legislative, regulatory, and other policy proposals that have privacy or civil liberties implications. Ensuring that DoD considers and addresses the privacy and civil liberties implications of all DoD regulations and policies, and will lead the agency's evaluation of the privacy and civil liberties implications of legislative proposals, congressional testimony, and other materials pursuant to OMB Circular No. A-19.

(2) Taking a central role in overseeing, coordinating, and facilitating DoD's privacy and civil liberties compliance efforts, consistent with applicable law, regulation, and policy.

(3) Managing privacy risks associated with any DoD activities that involve the creation, collection, use, process, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems. The SAOP's review of privacy risks will begin at the earliest planning and development stages of DoD actions and policies that involve PII, and continue throughout the life cycle of the programs or information systems. Appropriately managing privacy risks may require DoD to take steps beyond those required in law, regulation, and policy.

(4) In support of the DoD PCLO, ensure implementation of Sections 2000ee-1 and 2000ee-2 of Title 42, U.S.C., including:

(a) Appropriate consideration and protection of privacy and civil liberties in DoD operations, policies, procedures, guidelines, and issuances.

(b) Ensuring adequate procedures to respond to complaints alleging DoD violations of privacy or civil liberties.

(c) Coordination of semiannual reports on the activities of the DoD Privacy and Civil Liberties Programs to the appropriate congressional committees, the Privacy and Civil Liberties Oversight Board, and the Secretary of Defense.

b. Serves as the Chair of the Defense Data Integrity Board.

c. Serves as the Privacy Act Access and Amendment appellate authority for OSD, the Office of the Joint Chiefs of Staff, and the Combatant Commands when an individual is denied access to, or amendment of, records pursuant to the Privacy Act of 1974.

d. Submits the annual FISMA Privacy Report to the Department of Homeland Security and OMB in accordance with Chapter 35, Subchapter II, of Title 44, U.S.C.

e. In conjunction with the DoD Chief Information Officer (DoD CIO):

(1) Ensures DoD Components comply with OMB Circular No. A-130 with respect to the protection of PII.

(2) Ensures the DoD's breach response plan clearly defines the roles and responsibilities of DoD Component heads concerning contracts that:

(a) Involve the operation of a Privacy Act system of records;

(b) Involve the operation of federal information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII on behalf of the DoD; or

(c) Otherwise involve the maintenance of PII of DoD-affiliated personnel.

2.3. CHIEF, DPCLTD. Under the authority, direction, and control of the CMO, through the Director, DO&C, the Chief, DPCLTD:

a. Ensures that policies, procedures, and systems for protecting the privacy and civil liberties of individuals are implemented throughout the DoD in accordance with applicable law.

b. Oversees and implements the DoD Privacy and Civil Liberties Programs.

c. Ensures that guidance, assistance, and subject matter expert support are provided to the DoD Component PCLOs in the implementation and execution of the DoD Privacy and Civil Liberties Programs.

d. Assists the CMO and Director, DO&C, with the responsibilities outlined in Paragraphs 2.1 and 2.2.

e. Reviews legislative, regulatory, and other policy proposals with privacy and civil liberties implications, including those relating to how the DoD maintains its PII as well as proposed testimony in accordance with DoDD 5500.01.

f. Reviews proposed new and modified SORNs and proposed rescindment of SORNs. In accordance with the Privacy Act of 1974, OMB Circular No. A-108, and DoD 5400.11-R, ensures:

(1) Advance notification of such notices and rescindments to OMB and Congress.

(2) Publication of such notices and rescindments in the Federal Register (FR)

g. Reviews proposed DoD Component privacy exemption rules. In accordance with the Privacy Act of 1974, OMB Circular No. A-108, and DoD 5400.11-R, ensures:

(1) Advance notification of such exemption rules to OMB and Congress.

(2) Publication of such exemption rules in the FR.

h. Develops, coordinates, and maintains all DoD matching agreements. In accordance with the Privacy Act of 1974, OMB Circular No. A-108, and DoD 5400.11-R, ensures:

(1) Advance notification of such matching agreements to OMB and Congress.

(2) Publication of required matching notices in the FR.

i. Provides guidance, assistance, and support to the DoD Components in their implementation of the DoD Privacy and Civil Liberties Programs to ensure that all requirements developed to maintain PII conform to the DoD Privacy and Civil Liberties Programs standards.

j. Compiles data in support of the SAOP and DoD submissions for:

(1) The FISMA Annual Report, pursuant to OMB Memorandum M-17-12 and related OMB FISMA guidance.

(2) The Annual Matching Activity Report to OMB, in accordance with Section 552a(r) of Title 5, U.S.C., OMB Circular No. A-108, and DoD 5400.11-R.

(3) The Semi-annual DoD Privacy and Civil Liberties Officer (Section 803) Report in accordance with Section 2000ee-1 of Title 42, U.S.C.

(4) Other reports, as required.

k. Provides operational, logistical, and administrative support, including serving as the Executive Secretary to the Defense Data Integrity Board.

l. Establishes standards and reporting guidance for DoD Components for the management, reporting, and remediation of breaches of privacy information in accordance with OMB Memorandum M-17-12.

m. Develops standards and reporting guidance for DoD Components for the management and reporting of alleged violations of privacy and civil liberties, in accordance with the complaint procedures outlined by each DoD Component.

n. Ensures that the DoD has adequate procedures in place to receive, investigate, respond to, and redress complaints from individuals who allege that the DoD has violated their privacy or civil liberties.

o. On behalf of the Secretary of Defense, assigns periodic reports and data calls to DoD Components pursuant to OMB, the Privacy and Civil Liberties Oversight Board, and other statutory and regulatory requirements.

p. In conjunction with the DoD CIO, maintains an accurate inventory of DoD's information systems containing high-value assets (HVAs).

q. Serves as the approval authority for Social Security number (SSN) use and justification for all DoD and Secretary of Defense forms and DoD systems containing SSNs. Provides guidance to support DoD efforts in SSN collection, use, dissemination, and reduction in accordance with DoDI 1000.30 and Public Law 115-59, also known as the "Social Security Number Fraud Prevention Act of 2017."

2.4. GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE. In addition to the responsibilities in Paragraph 2.7., the General Counsel of the Department of Defense:

a. Provides advice and assistance on legal matters related to administering the DoD Privacy and Civil Liberties Programs.

b. Designates a representative from the Office of General Counsel of the Department of Defense to serve as a member of the Defense Data Integrity Board.

2.5. DOD CIO. In addition to the responsibilities in Paragraph 2.7., the DoD CIO:

a. Ensures the Chief Information Security Officer develops and maintains the DoD cybersecurity program in accordance with FISMA to protect PII.

b. In coordination with the Director, DO&C, reviews and approves the information technology (IT) investments budget request to ensure compliance with privacy risk management requirements.

c. Designates a representative from the Office of the DoD CIO to serve as a member of the Defense Data Integrity Board.

d. Facilitates exchange of information necessary to evaluate privacy risk associated with an information system's implementation of privacy and security controls, and any associated residual risk between the Chief Information Security Officer and the Director, DO&C.

2.6. INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE. In addition to the responsibilities in Paragraph 2.7., the Inspector General of the Department of Defense:

a. Reports privacy and civil liberties violations and their dispositions that are reported to the OIG DoD to DPCLTD in accordance with this issuance. Effective coordination and cooperation must not interfere with existing investigatory processes conducted by the OIG DoD, including investigations into privacy or civil liberties complaints.

b. Designates a representative from the OIG DoD to serve as a member of the Defense Data Integrity Board.

2.7. OSD PRINCIPAL STAFF ASSISTANTS. The OSD Principal Staff Assistants:

a. Appoint a senior member of their staff to serve as a Senior Component Official for Privacy (SCOP) to support the DoD SAOP in carrying out the SAOP's duties identified in OMB Circulars No. A-108 and No. A-130 and OMB Memorandum M-16-24.

(1) SCOPs appointed from the staffs of the OSD Principal Staff Assistants will serve primarily in an advisory capacity.

(2) In addition to attending periodic meetings conducted by the SAOP, these officials will oversee the functions described in Paragraph 3.1., and other activities designated by the SAOP.

b. May authorize written requests in accordance with Subsection (b)(7) of the Privacy of 1974, for records maintained by other federal or non-federal agencies that are necessary for an authorized law enforcement activity. This authorization may be delegated no lower than the section chief level.

2.8. DoD COMPONENT HEADS. The DoD Component heads:

a. Provide adequate resources to support and maintain effective privacy and civil liberties programs within their respective Components.

b. Ensure their Components comply with DoD Privacy and Civil Liberties Programs reporting requirements and supplemental guidance. Ensure procedures are in accordance with all applicable federal laws, regulations, policies, and procedures.

c. Designate a SCOP to support the DoD SAOP in carrying out the SAOP's duties identified in OMB Circulars No. A-108 and No. A-130, OMB Memorandum M-16-24, and Sections 2000ee-1 and 2000ee-2 of Title 42, U.S.C.

d. In consultation with the SCOP, designate DoD Component PCLOs to administer their Component's privacy and civil liberties programs.

e. Ensure DoD personnel and DoD contractors, who have primary responsibility for implementing the DoD Privacy and Civil Liberties Programs, receive appropriate privacy and civil liberties training. Define any such roles and responsibilities in applicable contracts, including privacy, security, and compliance controls contained in the Federal Acquisition Regulation and Defense Federal Acquisition Regulations.

f. Ensure that contracts requiring the operation of a system of records on behalf of DoD include provisions levying the requirements of the Privacy Act, as well as any other responsibilities concerning the protection of privacy and civil liberties. Ensure all DoD personnel and DoD contractors are trained on such responsibilities, in accordance with their positions and duties.

g. Evaluate all DoD Component legislative, regulatory, or other policy proposals for consistency with the privacy requirements of this issuance and DoD 5400.11-R.

h. Assess the impact of technology on privacy and the protection of PII and, when feasible, adopt privacy-enhancing technology and safeguards to:

(1) Safeguard PII contained in DoD Component Privacy Act systems of records.

(2) Collect and maintain the minimum amount of PII to accomplish the missions and functions of the DoD Component. This includes minimizing the collection and use of SSNs and complying with DoDI 1000.30.

(3) Audit compliance with the requirements of this issuance and DoD 5400.11-R.

(4) As appropriate, utilize the use of de-identification and/or anonymization technology to reduce risks to collections of PII.

i. Ensure that SCOPs and PCLOs periodically review DoD Component implementation of, and compliance with, the DoD Privacy and Civil Liberties Programs.

j. Comply with OMB Memorandum 17-12 and the DoD Breach Response Plan and establish and maintain formal breach response capabilities and mechanisms, implement formal incident management policies, and provide adequate training and awareness for employees and contractors on how to report, respond to, and mitigate incidents.

k. In coordination with the authorizing officials and SCOPs, implement a risk management framework to guide and inform the categorization of federal information and information systems; the selection, implementation, and assessment of privacy controls; the authorization of information systems; and the continuous monitoring of information systems.

l. When seeking IT investment funding, coordinate with their SCOP and their chief information officer to ensure necessary privacy risk management efforts are accounted for in the request.

m. As appropriate, authorize written requests pursuant to Subsection (b)(7) of the Privacy Act of 1974 for records maintained by other agencies that are necessary for an authorized law enforcement activity. This authorization may be delegated no lower than the section chief level.

n. Consult with SCOPs for privacy and civil liberties matters, as required by DoD Manual 5240.01.

2.9. SECRETARIES OF THE MILITARY DEPARTMENTS. In addition to the responsibilities in Paragraph 2.8., the Secretaries of the Military Departments program and budget to fund, without reimbursement, the administrative and logistic support required by Combatant Command and subordinate command headquarters to perform their assigned privacy and civil liberties missions as identified in DoDD 5100.03. As an exception to DoDD 5100.03, Combatant Commands, through their PCLOs, submit to the CMO, through DO&C, Component inputs to the FISMA Annual Report, the Semi-annual DoD Privacy and Civil Liberties Officer (Section 803) Reports, and other reports or data requested by the CMO.

SECTION 3: ROLE OF SCOPS AND PCLOS

3.1. DoD AND OSD COMPONENT SCOPs.

a. Table 1 lists the DoD and OSD Components that are supported by Washington Headquarters Services (WHS), Executive Services Directorate, Records, Privacy, and Declassification Division (RPDD). Such components are referred to in this issuance as the "WHS-serviced Components." WHS-serviced Components should report through RPDD.

Table 1. WHS-serviced Components

Immediate Office of the Secretary of Defense/Deputy Secretary of Defense
OSD Components
Office of the Assistant Secretary of Defense for Legislative Affairs
Office of the Director, Operational Test and Evaluation
Office of the DoD CIO
Office of the Chairman of the Joint Chiefs of Staff
Office of the CMO
Office of the Assistant to the Secretary of Defense for Public Affairs
Office of the Director, Cost Assessment and Program Evaluation
Office of the Director, Net Assessment
Office of the General Counsel of the Department of Defense
Office of the Under Secretary of Defense (OUSD) (Comptroller)/Chief Financial Officer, Department of Defense
OUSD for Acquisition and Sustainment
OUSD for Intelligence
OUSD for Personnel and Readiness
OUSD for Policy
OUSD for Research and Engineering

Table 1. WHS-serviced Components, Continued

DoD Components
Defense Acquisition University
Defense Advanced Research Projects Agency
Defense Legal Services Agency
Defense Media Activity
Defense Prisoners of War/Missing In Action Accounting Agency
Defense Security Cooperation Agency
Defense Technical Information Center
Defense Technology Security Administration
Department of Defense Education Activity
Department of Defense Human Resources Activity
Department of Defense Test Resource Management Center
National Defense University
Office of Economic Adjustment
Pentagon Force Protection Agency
WHS

b. The DoD SAOP has the authority to assign additional responsibilities to the SCOP as needed (e.g., in response to new statutory or regulatory requirements, or changes in policy from OMB). All DoD Component SCOPs, including the WHS-serviced Component SCOPs, will:

(1) Oversee and provide strategic direction for the respective component privacy and civil liberties programs.

(2) Provide advice and information to the DoD SAOP on privacy issues and civil liberties concerns within his or her respective Component.

(3) Ensure employee awareness of privacy and civil liberties and accompanying responsibilities to protect them.

c. In accordance with DoDI 8510.01 and in conjunction with the DoD Component senior information security officers and the Risk Management Framework Technical Advisory Group, all DoD Component SCOPs will:

(1) Review and approve the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII in accordance with Appendix F of Committee for National Security Systems Instruction No. 1253.

(2) Designate which privacy controls will be treated as program management, common, information system-specific, or hybrid privacy controls in the Component.

(3) Use the Privacy Overlay found in Attachment 6 of Appendix F of Committee for National Security Systems Instruction No. 1253 to select privacy and security controls for information systems containing PII. This will ensure the implementation of information security and privacy control measures at every stage in the life cycle.

(4) Review and approve the System Privacy Plans portion of the System Security Plan for Component information systems containing PII before authorization, reauthorization, or ongoing authorization.

(5) Identify assessment methodologies and metrics to determine whether privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and management of privacy risks.

(6) Identify and maintain inventory of HVAs, as defined in OMB Memorandum M-17-09.

(7) Coordinate with authorizing officials on granting authorization to operate decisions for information systems.

(8) Ensure that the DoD SAOP is aware of information systems and Component systems of records containing PII that cannot be appropriately protected or secured, and that such systems are given a high priority for upgrade, replacement, or retirement.

d. Implement the DoD Breach Response Plan and, as necessary, establish Component breach management policies. Ensure adequate training and awareness is provided to employees and contractors on how to report, respond to, and mitigate breaches of PII. For breaches involving protected health information, defer to the Defense Health Agency Privacy and Civil Liberties Office for direction under Public Law 104-191, also known as the "Health Insurance Portability and Accountability Act of 1996," and DoD 6025.18-R.

e. Ensure adequate procedures are in place for the management and remediation of both privacy and civil liberties complaints and alleged violations.

f. Review and approve reports as required for submission to the DPCLTD.

g. Establish as necessary a Component-level program to provide employee awareness of privacy and civil liberties as well as supervisor and senior-leader understanding of

responsibilities to protect privacy and civil liberties. The program must include and disseminate procedures for submitting and responding to complaints of violations.

3.2. DoD COMPONENT AND OSD PRINCIPAL STAFF ASSISTANT PCLOs. DoD Component and OSD Principal Staff Assistant PCLOs:

a. Manage and supervise the functions of the DoD Privacy and Civil Liberties Programs for their respective organizations.

b. Ensure appropriate administrative, physical, and technical safeguards and procedures are established for information systems that contain PII.

c. Collaborate, as necessary and appropriate, with information management, information collection, information security, forms and publications management, records management, chief information officer, and attorney and legal advisor staffs.

d. Aggregate data and submit reports to the Chief, DPCLTD, through their respective SCOPs. For WHS-serviced Components submit these reports through RPDD.

e. To the extent authorized by the Privacy Act of 1974 and using procedures outlined in Part 310 of Title 32, Code of Federal Regulations and the respective SORN:

(1) Process requests from individuals for access to records or to information pertaining to the individual from the DoD Component that maintains the system of records.

(2) Provide a copy of such records, in whole or in part, to the individual, unless such information should be withheld pursuant to applicable exemptions.

(3) Correct or amend such records if it has been determined by the DoD Component that the records are not accurate, relevant, timely, or complete, unless an exemption applies.

(4) Process appeals of denials of requests to access or amend a record.

f. Submit SORNs and exemption rules to the DPCLTD. For WHS-serviced Components, submit these documents through RPDD.

g. Implement formal breach management policies, and provide adequate training and awareness for employees and contractors on how to report and respond to breaches of PII.

h. Provide mechanisms for submitting privacy and civil liberties complaints or alleged violations, in accordance with DoD 5400.11-R.

i. Ensure employee awareness of methods to address allegations of privacy and civil liberties violations.

j. Review and coordinate with appropriate Component personnel DD Form 2930, “Privacy Impact Assessment (PIA),” available at http://www.esd.whs.mil/Directives/forms/, for information systems in accordance with DoDI 5400.16.

(1) This form must be used when developing, procuring, or using IT that collects maintains, or disseminates PII, or when collecting, maintaining or disseminating PII using IT, in accordance with Section 208 of Public Law 107-347, also known as the "E-Government Act of 2002."

(2) Make the privacy impact assessments available to the public in accordance with OMB policy and DoDI 5400.16. In accordance with DoDI 5400.16, if section 1 of DD Form 2930 contains information that would raise security concerns or reveal classified or sensitive information, the DoD Component can restrict the publication of the assessment.

k. Submit SSN reduction and justification memoranda to DPCLTD for final approval after the appropriate SCOP has signed them in accordance with Enclosure 3 of DoDI 1000.30. For WHS-serviced Components, submit these documents through RPDD.

l. Coordinate with the Defense Health Agency Privacy and Civil Liberties Office for all matters related to protected health information covered by Public Law 104-191, also known as the "Health Insurance Portability and Accountability Act of 1996."

m. Ensure component insider threat program officials include privacy and civil liberties in their training programs in accordance with DoDD 5205.16.

n. Coordinate with their appropriate legal office to advise heads of Defense Intelligence Components on privacy and civil liberties equities in accordance with DoD Manual 5240.01.

SECTION 4: DEFENSE DATA INTEGRITY BOARD

4.1. RESPONSIBILITIES. The Defense Data Integrity Board:

a. Reviews, approves, and maintains all written agreements for receiving or disclosing DoD records for matching programs to ensure compliance with the Privacy Act of 1974, as amended, and all relevant statutes, regulations, and guidelines.

b. Reviews all matching programs in which DoD has participated during the year, either as a source agency or recipient agency; determines compliance with applicable laws, regulations, guidelines, and agency agreements; and assesses the costs and benefits of such programs.

c. Reviews all recurring matching programs in which DoD has participated during the year, either as a source agency or recipient agency, for continued justification for such disclosures.

d. Compiles an annual report, which will be submitted to the DoD SAOP and OMB and made available to the public on request. This report will describe the matching activities in accordance with Subsection (u)(3)(D) of the Privacy Act of 1974, as amended, and OMB No. A-108 reflecting the matching activities in which DoD has participated in the previous year.

4.2. MEMBERSHIP. The Defense Data Integrity Board members must be full-time or permanent part-time government employees or Military Service members. The Board consists of:

a. Director, DO&C, who serves as the Chair.

b. Chief, DPCLTD, who serves as the Executive Secretary.

c. Military Department SCOPs.

d. Representative from DoD OCIO

e. Representative from the Office of General Counsel of the Department of Defense.

f. Representative from OIG DoD.

g. Director, Defense Manpower Data Center.

h. Deputy Director, Joint Service Provider

SECTION 5: DOD RULES OF CONDUCT

5.1. GENERAL. The DO&C establishes rules of conduct for DoD personnel involved in designing, developing, operating, or maintaining any system of records, or in maintaining any record in accordance with Section (e)(9) of the Privacy Act of 1974. DoD personnel must be trained, and must ensure that contractors are trained, with respect to such rules, the requirements of this section, and any other rules or procedures adopted pursuant to this section, including the penalties for noncompliance. More detailed training provisions are outlined in DoD 5400.11-R.

a. Consistent with applicable law, information about an individual that is collected, used, maintained, or disseminated by the DoD Components will be:

(1) Legally authorized, relevant, and necessary to accomplish an established DoD mission or function.

(2) Accurate, relevant, timely, and complete for its stated purpose.

(3) Collected directly from the individual to the greatest extent practicable when the information may result in adverse determinations about the individual's rights, benefits, and privileges. The individual will be informed of:

(a) The specific purpose or purposes for which the information is intended to be used.

(b) The authority for collection.

(c) How the PII may be used.

(d) Whether disclosing of such information is mandatory or voluntary.

(e) The consequences to the individual of not providing that information.

b. The records used in any determination about any individual will be maintained with such accuracy, relevancy, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination.

c. DoD Components will establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

d. DoD Components will make reasonable efforts to ensure records are accurate, timely, and relevant for DoD's purposes before disseminating any record about an individual to any person or to another federal or non-federal agency. This requirement does not apply if the record is being released pursuant to Section 552 of Title 5, U.S.C., also known and referred to in this issuance as the "Freedom of Information Act."

e. Disclosing records pertaining to an individual from a system of records is prohibited in the absence of the individual's consent except as authorized by the Privacy Act of 1974 and the Freedom of Information Act.

f. Pursuant to the Privacy Act of 1974, no record will be maintained on how an individual exercises rights guaranteed by the First Amendment to the United States Constitution, except:

(1) When expressly authorized by statute.

(2) When expressly authorized by the individual who is the subject of the record.

(3) When the record is pertinent to and within the scope of an authorized law enforcement activity.

g. Protected health information will be disclosed in accordance with DoD 6025.18-R or its successor issuance. Questions regarding the disclosure of protected health information should be referred to the Defense Health Agency Privacy and Civil Liberties Office.

h. DoD Components will report any unauthorized disclosures of PII from a system of records to the applicable SCOP or PCLO.

5.2. FAIR INFORMATION PRACTICE PRINCIPLES (FIPPs). DoD Components are expected to consider the FIPPS when evaluating information systems, processes, programs, and activities that affect individual privacy consistent with the DoD mission and privacy program requirements. To the extent a particular principle cannot be implemented, other principles should be used to compensate for the privacy and civil liberties risks identified. For the purposes of this issuance, the FIPPs are:

a. Access and Amendment. Provide individuals with appropriate access to PII and appropriate opportunity to correct or amend PII.

b. Accountability. Hold personnel accountable for complying with measures that implement the FIPPs and applicable privacy requirements, and appropriately monitor, audit, and document compliance. Clearly define the roles and responsibilities with respect to PII for all employees and contractors, and provide appropriate training to all employees and contractors who have access to PII.

c. Authority. Create, collect, use, process, store, maintain, disseminate, or disclose PII only with the proper authority to do so and identify this authority in the appropriate notice.

d. Minimization. Create, collect, use, process, store, maintain, disseminate, or disclose PII only when it is directly relevant and necessary to accomplish a legally authorized purpose, and only maintain PII for as long as is necessary to accomplish the purpose.

e. Quality and Integrity. Create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.

f. Individual Participation. Involve the individual in the process of using PII and, to the extent practicable, seek individual consent for creating, collecting, using, processing, storing, maintaining, disseminating, or disclosing PII. Establish procedures to receive and address individuals' privacy-related complaints and inquiries.

g. Purpose Specification and Use Limitation. Specify the purpose for which PII is collected and only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the public notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.

h. Security. Establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.

i. Transparency. Be transparent about information policies and practices with respect to PII, and provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

GLOSSARY

G.1. ACRONYMS.

CMO	Chief Management Officer of the Department of Defense
DoD CIO	DoD Chief Information Officer
DO&C	Directorate for Oversight and Compliance
DoDD	DoD directive
DoDI	DoD instruction
DPCLTD	Defense Privacy, Civil Liberties, and Transparency Division
FIPPs	Fair Information Practice Principles
FISMA	Federal Information Security Management Act
FR	Federal Register
HVA	high-value asset
IT	information technology
OIG DoD	Office of the Inspector General of the Department of Defense
OMB	Office of Management and Budget
OUSD	Office of the Under Secretary of Defense
PCLO	privacy and civil liberties officer
PIA	privacy impact assessment
PII	personally identifiable information
RPDD	Records, Privacy, and Declassification Division
SAOP	Senior Agency Official for Privacy
SCOP	Senior Component Official for Privacy
SORN	system of records notice
SSN	Social Security number
U.S.C.	United States Code
WHS	Washington Headquarters Services

G.2. DEFINITIONS. Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

breach. Defined in OMB Memorandum M-17-12.

civil liberties. Fundamental rights and freedoms protected by the United States Constitution.

complaint. An assertion alleging a violation of privacy or civil liberties.

disclosure. The information sharing or transfer of any PII from a system of records by any means of communication (such as oral, written, electronic, or other) to any person, entity, or forum, other than the subject of the record, the subject's designated agent, or the subject's legal guardian.

DoD contractor. Any person or other legal entity that directly or indirectly (e.g., through an affiliate) is awarded a government contract. This may include a contract for carriage under government or commercial bills of lading, or a subcontract under a government contract. A DoD contractor includes a contractor who conducts business with the Federal Government as an agent or representative of another contractor.

DoD personnel. Service members and federal civilian employees.

HVAs. Defined in OMB M-17-09.

individual. Defined in the Privacy Act of 1974.

maintain. Defined in the Privacy Act of 1974.

matching program. Defined in the Privacy Act of 1974.

PII. Defined in OMB Circular No. A-130.

PCLO. A federal employee who is responsible for the day-to-day management of the DoD Component privacy and civil liberties programs.

protected health information. Defined in DoD 6025.18-R.

record. Defined in the Privacy Act of 1974.

SCOP. A member of the Senior Executive Service, a Senior Level employee, or general officer or flag officer responsible for the overall implementation of the privacy and civil liberties programs in his or her DoD Component.

SORN. Defined in OMB Circular No. A-108.

system of records. Defined in the Privacy Act of 1974.

violation of civil liberties. Undue interference with the exercise of civil liberties.

REFERENCES

Committee for National Security Systems Instruction No. 1253, Appendix F, Attachment 6, "Privacy Overlay," April 23, 2015

Deputy Secretary of Defense Memorandum, "Reorganization of the Office of the Deputy Chief Management Officer," July 11, 2014

DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007

DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 24, 2003

DoD Directive 5100.03, "Support of The Headquarters of Combatant and Subordinate Unified Commands," February 9, 2011, as amended

DoD Directive 5105.53, "Director of Administration and Management (DA&M)," February 26, 2008

DoD Directive 5105.82, "Deputy Chief Management Officer (DCMO) of the Department of Defense," October 17, 2008

DoD Directive 5205.16, "The DoD Insider Threat Program," September 30, 2014, as amended

DoD Directive 5500.01, "Preparing, Processing, and Coordinating Legislation, Executive Orders, Proclamations, Views Letters, and Testimony," June 15, 2007

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

DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," July 14, 2015, as amended

DoD Instruction 5545.02, "DoD Policy for Congressional Authorization and Appropriations Reporting Requirements," December 19, 2008

DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended

DoD Manual 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities," August 8, 2016

DoD Manual 8910.01, Volume 1, "DoD Information Collections Manual: Procedures for DoD Internal Information Collections," June 30, 2014, as amended

Executive Order 12,333, "United States Intelligence activities," December 4, 1981

Office of the Deputy Chief Management Officer Memorandum, "DoD Breach Response Plan," September 28, 2017[1]

Office of Management and Budget Circular A-19, "Legislative Coordination and Clearance," Revised September 20, 1979

Office of Management and Budget Circular A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," December 23, 2016

Office of Management and Budget Circular A-130, "Managing Information as a Strategic Resource," July 27, 2016

Office of Management and Budget Memorandum M-16-24, "Role and Designation of Senior Agency Officials for Privacy," September 15, 2016

[1] This memorandum may be requested via email osd.ncr.odcmo.mbx.dpcld-correspondence@mail.mil.

Office of Management and Budget Memorandum M-17-09, "Management of Federal High Value Assets," December 9, 2016

Office of Management and Budget Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," January 3, 2017

Public Law 104-191, "Health Insurance Portability and Accountability Act of 1996 (HIPAA)," August 21, 1996

Public Law 107-347, Section 208, "E-Government Act of 2002," December 17, 2002

Public Law 115-59, "Social Security Number Fraud Prevention Act of 2017," September 15, 2017

Secretary of Defense Memorandum, "Disestablishment of the Deputy Chief Management Officer and Establishment of the Chief Management Officer," February 1, 2018

United States Code, Title 5

United States Code, Title 42

United States Code, Title 44, Chapter 35, Subchapter II (also known as the "Federal Information Security Modernization Act of 2014")

United States Constitution