DCMA Manual 4502-13

Privacy and Civil Liberties

==========

Office of Primary Responsibility	**Corporate Governance Capability**
Effective:	March 14, 2019
Releasability:	Cleared for public release
New Issuance	
Implements:	DCMA-INST 4502, "Corporate Governance," January 14, 2019
Internal Control:	Process flow and key controls are located on the Resource Page
Labor Codes:	Located on the Resource Page
Resource Page Link:	https://360.dcma.mil/sites/policy/CG/SitePages/4502-13r.aspx
Approved by:	David H. Lewis, VADM, USN, Director

Purpose: In accordance with the authority in DoD Directive 5105.64, "Defense Contract Management Agency (DCMA)," this Manual establishes the procedures and assigns responsibilities for implementing the policy in DCMA Instruction 4502.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. This issuance applies to all DCMA personnel.

b. The Federal Acquisition Regulation (FAR), Subparts 24.1, "Protection of Individual Privacy," and 24.3, "Privacy Training," apply to DCMA contractors.

1.2. POLICY. It is DCMA policy to:

a. Protect individuals' privacy and civil liberties rights, consistent with federal laws, regulations, and policies.

b. Minimize collection of personally identifiable information (PII) within published and authorized systems of records, and maintain only PII that is required to accomplish DCMA's mission.

c. Minimize collection, use, maintenance, and dissemination of information about individuals for purposes of discharging DCMA's statutory responsibilities, when possible and practicable.

d. Protect improper release of information that is protected by federal laws, regulations and policies.

e. Execute this manual in a safe, efficient, effective, and ethical manner.

SECTION 2: RESPONSIBILITIES

2.1. DIRECTOR, DCMA. The Director, DCMA will:

a. Provide adequate funding and personnel to establish and support an effective DCMA Privacy and Civil Liberties Program.

b. Ensure DCMA compliance with DoD Privacy and Civil Liberties Program reporting requirements, supplemental guidance, and procedures in accordance with all applicable federal laws, regulations, policies, and procedures.

c. Designate a DCMA Senior Component Official for Privacy (SCOP) in writing and notify the Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD) of that designation.

d. Designate a DCMA Privacy and Civil Liberties Officer (PCLO) in writing and notify DPCLTD of that designation.

e. Approve System of Records Notices (SORNs).

f. Ensure DCMA personnel and contractors who have primary responsibility for implementing the DCMA Privacy and Civil Liberties Program receive appropriate privacy and civil liberties training. This training must be consistent with the requirements of DoD 5400.11-R, "Department of Defense Privacy Program," and address the provisions of DoD Directive (DoDD) 5400.11, "DoD Privacy Program," Section 552a of Title 5, United States Code (U.S.C.), also known and referred to in this manual as "the Privacy Act (PA)," and Office of Management and Budget (OMB) Circulars A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication Under the Privacy Act," and A-130, "Managing Information as a Strategic Resource."

g. Ensure all DCMA personnel and contractors are trained on their responsibilities under the PA and on their responsibilities concerning protection of civil liberties, in accordance with their positions and duties.

h. Ensure all DCMA legislative, regulatory, or other policy proposals are evaluated to ensure consistency with DoD 5400.11-R and DoDD 5400.11.

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

(1) Preserve and protect PII contained in DCMA systems of records.

(2) Collect and maintain the minimum amount of PII to accomplish DCMA missions and functions.

2.2. SENIOR COMPONENT OFFICIAL FOR PRIVACY. The SCOP will:

a. Serve as principal advisor on all Agency privacy and civil liberties matters, to include program oversight, administration, and implementation of best practices.

b. Administer the program through the PCLO, who will serve as the principal program manager for the Agency.

c. Review and approve for submission to DoD all Privacy and Civil Liberties recurring reports as listed in Section 8 of this manual and any ad hoc reports as required by the DPCLTD.

d. Provide advice and information to the DoD Senior Agency Official for Privacy (SAOP) on privacy issues and civil liberties concerns within DCMA.

e. Review proposed new and modified SORNs, notices of SORN rescindment, privacy exemption rules, and Privacy Impact Assessments (PIAs).

f. Submit SORNs to Director, DCMA for approval.

g. Submit approved SORNs to DPCLTD for publication in the Federal Register (FR).

h. Coordinate with authorizing officials on granting Authority to Operate decisions for information systems.

i. Coordinate with DCMA Information Technology (IT) system security controls assessors on several issues associated with privacy controls and plans related to information systems, as listed in the August 28, 2017 Office of the Deputy Chief Management Officer Memorandum, "Designation of Senior Component Officials for Privacy and Establishment of Roles and Responsibilities."

j. Ensure the DoD SAOP is made aware of information systems and components that cannot be appropriately protected or secured, and that the Component ensures such systems are given a high priority for upgrade, replacement, or retirement.

k. Implement the DoD breach response plan and, as necessary, establish DCMA breach management policies, and ensure adequate training and awareness is provided to employees and contractors on how to report and respond to breaches of PII.

l. Ensure adequate procedures are in place for the management and remediation of civil liberties complaints.

m. Ensure employee awareness of civil liberties, including procedures for submitting and responding to complaints of violations.

n. Ensure supervisor and senior leaders understanding of the responsibility to protect the civil liberties for personnel within the scope of their authority.

2.3. PRIVACY AND CIVIL LIBERTIES OFFICER. The PCLO will:

a. Manage the DCMA Privacy and Civil Liberties Program.

b. Implement processes to receive and adjudicate privacy and civil liberties complaints.

c. Provide for the adequate training and awareness for employees and contractors on how to report and respond to breaches of PII.

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

e. Ensure the establishment of appropriate administrative, physical, and technical safeguards and procedures for information systems which contain PII.

f. Coordinate with appropriate information management and records management staffs.

g. Aggregate data and submit reports to the DPCLTD through the DCMA SCOP.

h. In coordination with DCMA IT, support DCMA components and/or business capabilities in the development of PIA for systems of records under those components' responsibility by providing guidance, training, and other help as needed.

i. Develop SORNs in coordination with DCMA IT and the DCMA components and/or business capabilities applicable to the system of records.

2.4. COMPONENT HEADS AND/OR CAPABILITY MANAGERS. Component Heads and/or Capability Managers will:

a. Assist the DCMA PCLO in investigating privacy and civil liberties complaints that pertain to their employees and organization.

b. Ensure they or their staff have completed the required training applicable to privacy and civil liberties, which is listed on the resource page for this manual.

c. For systems of records under their cognizance, they will:

(1) Ensure a current Federal Government, DoD, or Agency SORN covers each of the system(s) of records.

(2) Ensure there is a need and relevancy to collect privacy data within the system of records, providing justification for the use of the Social Security Number (SSN), if necessary.

(3) Identify the required controls and individuals authorized access to PII and periodically review and update the identification of individuals who require authorization to access the system of records.

(4) Establish appropriate administrative, technical, and physical safeguards to ensure records in the system of records are protected from unauthorized alteration, destruction, or disclosure, which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is maintained.

(5) Ensure employees have read and agreed to abide by the Rules of Conduct in paragraph 3.5. for the information and information systems for which they require access prior to being granted access, pursuant to OMB Circular A-130. Ensure all personnel who have access to the system of records, or who are engaged in developing or supervising procedures for handling records, are fully aware of their responsibilities to protect personal information established by the Agency Privacy and Civil Liberties program.

(6) Maintain an accurate record of any disclosures, including the date of the disclosure, a description of the information disclosed, the purpose of the disclosure, and the name and address of the person or agency to whom the disclosure was made. This includes disclosures made with the consent of the affected individual, but not those made to DoD personnel for use in performing their official duties or those made under the Freedom of Information Act (FOIA).

(7) Conduct periodic reviews of the system of records as required by OMB Circular A-130.

(8) Ensure adherence to all other privacy and civil liberties requirements as laid out in applicable federal, DoD and DCMA laws, regulations, policies, and procedures.

2.5. GENERAL COUNSEL (GC). In addition to the requirements listed in paragraph 2.4., the GC will:

a. Provide advice and assistance on legal matters related to the administration of the DCMA Privacy and Civil Liberties Program.

b. Inform and advise the SCOP and PCLO on privacy and civil liberties related litigation, judicial decisions, legislation, and other legal issuances or developments that affect the administration of the program.

c. Review allegations of privacy and/or civil liberties violations and provide support to the investigations of those allegations, as appropriate.

d. Review SORNs and PIAs.

e. Review notifications to individuals affected by the loss, theft, or compromise of PII.

2.6. EXECUTIVE DIRECTOR, CORPORATE OPERATIONS (DC). In addition to the responsibilities listed in paragraph 2.4., the Executive Director, DC, will:

a. Provide oversight for the Privacy and Civil Liberties Program through the Director of Strategic Communication (DCC).

b. Review and approve the reports listed in Section 7.

2.7. EXECUTIVE DIRECTOR, IT AND CHIEF INFORMATION OFFICER (CIO). In addition to the responsibilities listed in paragraph 2.4., the Executive Director, IT/CIO will:

a. Serve as the DCMA PIA approval official with the responsibility to review, approve, and submit all DCMA PIAs to DoD and OMB according to Federal and DoD guidance.

b. Oversee DCMA PIA policy and procedures to ensure PIAs are conducted commensurate with the information system being assessed, the sensitivity of information in the system, and the risk of harm for unauthorized release of that information in accordance with DoD Instruction (DoDI) 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance."

c. Coordinate SORN development with the DCMA SCOP/PCLO and the DCMA components and/or business capabilities applicable to the system of records.

d. Ensure a current Federal Government, DoD, or Agency SORN covers all DCMA systems of record.

e. Ensure the integration of PII protection into the overall DCMA major information system life cycle management process.

f. Provide guidance for effective assessment, utilization, and management of privacy-related technologies to include establishing and validating Agency information systems privacy requirements.

g. Provide guidance on the use of encryption software to protect privacy sensitive information.

h. Serve as the focal point in establishing and validating Agency web privacy requirements and policy.

2.8. DIRECTOR, TOTAL WORKFORCE. In addition to the responsibilities listed in paragraph 2.4., the Total Workforce Director will report to the PCLO any alleged violations of privacy and/or civil liberties.

2.9. DIRECTOR, EQUAL EMPLOYMENT OPPORTUNITY (EEO). In addition to the responsibilities listed in paragraph 2.4., the Director, EEO will report to the PCLO any alleged violations of privacy and/or civil liberties.

2.10. DCMA PERSONNEL. DCMA personnel will:

a. Uphold the Rules of Conduct listed in Section 4 of this manual.

b. Complete Privacy and Civil Liberties training annually via the courses listed on the resource page for this manual.

c. Take appropriate precautions in accordance with the PA when:

(1) Collecting personal information; ensuring appropriate safeguards are in place to protect the privacy and civil liberties of individuals.

(2) Creating and/or maintaining records containing PII.

(3) Disseminating information containing personal data.

d. Report suspected privacy and/or civil liberties issues to the PCLO in accordance with the protocol established by the resource page for this manual.

SECTION 3: GENERAL PRINCIPLES

3.1. DOD PRINCIPLES OF PRIVACY AND CIVIL LIBERTIES.

a. The privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies.

b. The increasing use of computers and sophisticated IT, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information.

c. The opportunities for an individual to secure employment, insurance, and credit, and his or her right to due process, and other legal protections are endangered by the misuse of certain information systems.

d. Privacy rights and civil liberties are personal and fundamental rights protected by the Constitution of the United States, federal statutes and regulations.

e. In order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

3.2. PROGRAM OVERVIEW.

a. The PA establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of PII about individuals that is maintained in systems of records by federal agencies. The PA also provides individuals with a means by which to seek access to and amendment of their records, and sets forth various agency recordkeeping requirements.

b. Civil Liberties include the freedom of speech, assembly, press, and religion. Employees must recognize and protect the civil liberties of DoD employees, members of the military services, and the public to the greatest extent possible.

c. The government's need to maintain information must be weighed with the obligation to protect individuals against unwarranted invasions of their privacy stemming from the Agency's collection, maintenance, use, and disclosure of PII.

d. Appropriate administrative, technical, and physical safeguarding methods must be utilized to protect the PII of all U.S. citizens and legally admitted aliens. The IT environment subjects PII to special hazards as to unauthorized compromise, alteration, dissemination, and use. Therefore, additional considerations must be given to safeguarding PII in IT systems, in accordance with DoD 5400.11-R, DoDI 5400.16, and DoDI 8580.02, "Security of Individually Identifiable Health Information in DoD Health Care Programs,"and Agency requirements.

3.3. FAIR INFORMATION PRACTICES PRINCIPLES (FIPPS). FIPPs should be considered when evaluating information systems, processes, programs, and activities that affect individual privacy in accordance with the DoD mission and privacy program requirements. For the purposes of this manual, the FIPPs are:

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

b. Accountability. Be accountable for complying with these principles 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 who have access to PII.

c. Authority. Create, collect, use, process, store, maintain, disseminate, or disclose PII only if 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 that is directly relevant and necessary to accomplish a legally authorized purpose, and should 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. Provide notice of the specific purpose for which PII is collected and only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the 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 provides clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

3.4. DCMA PRIVACY AND CIVIL LIBERTIES PROGRAM OBJECTIVES. The primary objectives of the Privacy and Civil Liberties Program are to provide advice, monitoring, official reporting, and training as follows:

a. Privacy and civil liberties concerns must be considered when proposing, developing, and/or implementing policies, procedures, or guidelines related to the DCMA mission.

b. Periodic assessments of DCMA policies, procedures, and/or guidelines must be conducted to ensure that privacy and civil liberties concerns are adequately considered.

c. Adequate procedures must be in place to receive, investigate, respond to, and redress complaints from individuals alleging violations of privacy and/or civil liberties.

d. Privacy and civil liberties training modules must be developed and implemented as appropriate.

e. Transparent relationships with DCMA personnel, DCMA contractors, and the public must be maintained to communicate the role privacy and civil liberties play in the DCMA mission.

3.5. RULES OF CONDUCT. In accordance with Section (e) (9) of the PA, this paragraph provides DCMA Rules of Conduct for the development, operation, and maintenance of systems of records that contain PII. DCMA personnel will:

a. Take action to ensure that any PII contained in a system of records accessed and used by the employee to conduct official business will be protected so that the security and confidentiality of the information is preserved.

b. Not disclose any PII contained in any system of records, except as authorized by the PA or other applicable statute, executive order, regulation, or policy. Knowingly and willfully making an unlawful or unauthorized disclosure may result in criminal penalties or administrative sanctions.

c. Report any unauthorized disclosures of PII from a system of records to the PCLO.

d. Report the maintenance of any system of records not authorized by this manual to the PCLO.

e. Minimize the collection of PII to information that is relevant and necessary to accomplish the mission of DCMA.

f. Not maintain records describing how any individual exercises rights guaranteed by the First Amendment, except:

(1) When specifically authorized by statute;

(2) When expressly authorized by the individual that the record is about; or

(3) When the record is pertinent to and within the scope of an authorized law enforcement activity, including authorized intelligence or administrative activities.

g. Safeguard the privacy of all individuals and the confidentiality of all PII.

h. Limit the availability of records containing PII to DCMA personnel and DCMA contractors who have a need to know in order to perform their duties.

i. Prohibit unlawful possession, collection, or disclosure of PII, whether or not it is within a system of records.

j. Ensure that all DCMA personnel and DCMA contractors who either have access to a system of records or develop or supervise procedures for handling records in a system of records are aware of their responsibilities and are properly trained to safeguard PII being maintained under the DCMA Privacy and Civil Liberties Program.

k. Prepare any required new, amended, or altered SORN for a given system of records and submit the SORN through the PCLO to the Director, DPCLTD, for coordination and submission for publication in the FR.

l. Not maintain an unauthorized system of records, which is a system from which information is retrieved by an individual's name or other unique identifier. Any official who knowingly and willfully maintains a system of records without satisfying publication requirements as described in this manual (see paragraph 4.1.) and the PA may be subject to administrative sanctions or criminal penalties.

m. Maintain all records in a mixed system of records as if all the records in such a system are subject to the PA.

SECTION 4: HANDLING AND SAFEGUARDING PRIVACY DATA

4.1. SYSTEM OF RECORDS NOTICE.

a. Identifying the Need for a SORN. Records must be retrieved by name or other personal identifier to become a system of records, and a system notice must be submitted in accordance with DoD 5400.11-R. The system must be designed to retrieve information by personal identifier as a matter of practice. The fact that the system has the capability of retrieval (i.e., search capabilities) is not a qualifying factor in determining the need for a SORN. The Component Head/Capability Manager must identify the specific statute or the Executive Order that authorizes maintaining personal information in each system of records. Specific requirements for contents of the SORN are provided in DoD 5400.11-R. An existing Federal Government, DoD, or Agency SORN may be used if it properly covers the system of records being established or evaluated. Existing SORNs may be accessed through the resource page for this manual.

b. Evaluation of System of Records. The Component Head/Capability Manager will evaluate the information to be included in each new system before establishing the system, and evaluate periodically the information contained in each existing system of records for relevancy and necessity. Such a review will also occur when a system notice alteration or amendment is prepared. Consider all requirements as documented in DoD 5400.11-R, subparagraph C1.1.6.

c. Discontinued Information Requirements. Collection of any category or item of personal information for which retention is no longer justified should be stopped immediately. The information must be deleted immediately from existing records, when feasible. Do not destroy any records that must be retained in accordance with disposal authorizations established under Section 3303a of Title 44, U.S.C.

d. FR Publication. SORNs are published in the FR, in accordance with the PA, OMB Circulars A-108 and A-130, and DoD 5400.11-R. A new system of records must satisfy the SORN publication and review requirements before collecting or maintaining information about individuals for that system of records. Administrative Instruction (AI) No. 102, "Office of the Secretary of Defense (OSD) Federal Register (FR) System," provides information pertaining to the preparation of documents for publication in the FR. Publication of a document in the FR constitutes official public notice of the existence and content for the document. Procedures and requirements are specifically documented in DoD 5400.11-R, paragraph C6.1.

4.2. Privacy Impact Assessment (PIA). A PIA is an analysis of how PII is collected, used, shared, and maintained. The purpose of a PIA is to demonstrate that program managers and system owners consciously incorporated privacy protections throughout the development life cycle of a system or program. PIAs are required by the E-Government Act of 2002, which was enacted by Congress in order to improve the management and promotion of Federal electronic government services and processes. PIAs allow clear communication with the public about how DCMA handles information, including how the Agency addresses privacy concerns and safeguards information. Specific requirements for contents of a PIA are provided in DoD 5400.11-R.

4.3. COLLECTING PRIVACY DATA. DCMA recognizes that an individual's privacy and civil liberties are fundamental legal rights that must be respected and protected and requires all Agency personnel to conduct themselves consistent with the established rules of conduct in Section 4. It is the responsibility of each and every employee to be aware of their individual responsibilities when collecting, storing, sharing, handling, transmitting, and disposing of information protected by the Privacy and Civil Liberties Program. The "Privacy Act Data Cover Sheet" (DD Form 2923) must be used to safeguard and protect information containing PII.

a. Collecting Privacy Data. To the greatest extent practicable, personal information is to be collected directly from the individual to whom it pertains if the information may be used in making any determination about the rights, privileges, or benefits of the individual under any Federal program. The following represent examples where it may not be practical to collect personal information directly from an individual:

(1) Verifying information through third party sources for security or employment suitability determinations;

(2) Seeking third party opinions such as supervisory comments as to job knowledge, duty performance, or other opinion-type evaluations;

(3) Obtaining the needed information directly from the individual is exceptionally difficult or may result in unreasonable costs; or

(4) Contacting a third party at the request of the individual to furnish certain information such as exact periods of employment, termination dates, copies of records, or similar information.

b. Collecting SSNs. It is unlawful to deny an individual any right, benefit, or privilege provided by law because the individual refuses to provide his or her SSN. When an individual is requested to provide his or her SSN, procedures, as documented in DoD 5400.11-R, subparagraph C2.1.2, will be followed.

c. Privacy Act Statement (PAS). When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, a PAS is required regardless of the medium used to collect the information (paper or electronic forms, personal interviews, telephone interviews, or other methods). Requirements of the PAS are documented in DoD 5400.11-R, subparagraph C2.1.4. An example of a PAS is on the resource page for this manual.

d. Sharing Privacy Data. The "need-to-know" principle must be followed when sharing PII.. A need to know is established when a prospective recipient requires access to specific information in order to perform or assist in a lawful and authorized government function.

(1) PII may be shared with DCMA civilians, military service members, and/or DCMA contractors only when the data is needed to perform official, assigned duties.

(2) Share PII only with those individuals and entities that are listed in the "Routine Use" and disclosure clause of the governing SORN. (If it is not clear which SORN governs the system of records, contact the PCLO.)

(3) Interoffice envelopes or messenger-type envelopes should never be used unless the material is placed in an inner, sealed envelope and marked "For Official Use Only (FOUO) – Contains Privacy and Civil Liberties Program Protected Information."

(4) Disclosure of personal information to other agencies and third parties is detailed in Chapter 4 of DoD 5400.11-R.

e. Transmitting Privacy Data.

(1) Email.

(a) State that the email contains PII protected information in the opening line and in the last line of text "FOUO – Contains Privacy and Civil Liberties Protected Information."

(b) Never send mass mailings or "Reply to all" when an email contains PII protected information unless there is an official need for all addressees to receive the information.

(c) Digitally sign and encrypt all emails containing PII.

(d) Exercise caution when attaching documents containing PII to ensure that unnecessary and/or hidden information is properly redacted, sanitized, or extracted. Procedures for properly taking those actions may be found on the resource page for this manual.

(2) Facsimile (fax).

(a) Use a fax cover sheet that clearly indicates the name of the recipient and that the fax contains PII data.

(b) Call the intended recipient to ensure prompt pickup prior to faxing a documenting containing PII to an unsecured fax in a common area (or if you are uncertain as to the security of the receiving fax machine.)

(3) U.S. Mail or Commercial Shipping.

(a) Utilize existing tracking processes that allow a sender and recipient to sign for and verify delivery.

(b) Double wrap the package, using inner and outer envelopes as appropriate.

1. The inner envelope must be marked with detailed contact information for both the sender and recipient and "FOUO – Contains Privacy and Civil Liberties Program Protected Information."

2. The outer envelope must never include markings that the contents contain PII.

f. Printing Privacy Data. When printing PII, employees must:

(1) Retrieve documents immediately to avoid PII being left unattended at the copier.

(2) Exercise caution when printing, making certain the correct printer is selected.

g. Storing Privacy Data. Caution must be exercised when storing PII.

(1) The DoD Privacy Act Data Cover Sheet will be used. The cover sheet is available on the resource page for this manual.

(2) During duty hours, documents containing PII should be covered, turned upside down, placed in an out-of-sight location, or otherwise shielded from view when not being used or when individuals having no need for access to that data enter the work space.

(3) After duty hours, records containing PII should be placed in closed drawers or cabinets.

(4) Special categories of PII (i.e., medical files, investigative files, adverse action files) should be placed in locked offices, drawers or cabinets.

h. Records Disposal. Dispose of records containing personal data so as to prevent inadvertent compromise. For paper records, shredding is acceptable. For electronic records and media, overwriting, degaussing, shredding, and/or sanding are acceptable. Disposal methods are considered adequate if the personal data is rendered unrecognizable or beyond reconstruction.

4.4. LOST, STOLEN, OR COMPROMISED INFORMATION. If records containing PII are lost, stolen, or compromised, the potential exists that the records may be used for unlawful purposes, such as identity theft, fraud, stalking, etc. The personal impact on the affected individual(s) may be severe if the records are misused.

a. Breach vs. Incident. A "breach" occurs when protected information has been compromised, disclosed, or acquired without authorization and the Agency has lost control over the use of the information. A breach is distinguished from an "incident," which occurs when protected information remains under the control of the Agency, but the integrity or confidentiality of the information is compromised or jeopardized without authorization. The key distinguishing point between a breach and an incident is that the Agency retains control of the protected information. For example, the unauthorized disclosure of a document containing PII with a third party would be a breach. The posting of the document on DCMA's intranet where it

is available only to DCMA employees, rather than only DCMA employees with a need-to-know, would be an incident because DCMA has maintained control of the information.

b. Actions Upon Discovery of a Breach.

(1) All breaches will be reported immediately. The person discovering a breach will report it to the PCLO and, if known, the Component Head/Capability Manager with cognizance over the information system that was breached within 24 hours.

(2) The PCLO will notify the SCOP and CIO immediately and will notify DPCLTD and the U.S. Computer Emergency Readiness Team (USCERT) of the breach within 48 hours upon being notified.

(3) The notification process of DPCLTD and USCERT are described on the resource page for this manual.

(4) The notifications will include as much of the following information as able to be determined and be able to meet the 24- and 48-hour deadlines. Deadlines of the reporting takes precedence over details in the reports.

(a) Identify the DCMA component involved.

(b) The date of the breach.

(c) If known, or can be reasonably estimated, the number of individuals impacted, to include whether they are DoD civilian, military, or contractor personnel; DoD civilian or military retirees; family members; other Federal personnel or members of the public, etc.

(d) A description of the facts and circumstances surrounding the loss, theft, or compromise.

(e) A brief description of immediate actions taken in response to the breach, including:

1. Whether the incident was investigated or is being investigated.

2. Who led or is leading the investigation.

3. The final or preliminary results of the inquiry.

4. Actions taken to mitigate any harm that could result from the breach.

5. Whether the affected individuals are being notified.

6. What remedial actions have been or will be taken to prevent a similar breach in the future; e.g., refresher training conducted, new or revised guidance issued, and any other information considered pertinent as to ensure that information is properly safeguarded.

(5) The Component Head/Capability Manager for the breached system will continue determining as much as possible of the information listed in paragraph 4.4.b.(4).

c. Notification of Affected Individuals.

(1) Individuals affected by the loss, theft, or compromise of PII will be notified by the SCOP within 10 working days of when the Component Head/Capability Manager is able to determine the identities of the affected individuals. The Component Head/Capability Manager will submit the notification to the PCLO for review, who will coordinate with GC for a legal analysis of the proposed notification prior to submitting to the SCOP for approval and signature. The applicable Component Head/Capability Manager will support the SCOP in making the notifications.

(2) If only some, but possibly not all, of the affected individuals can be identified in time to meet the 10 working day notification deadline, then those who can be identified will be notified. Those individuals who are subsequently identified will be notified expeditiously.

(3) If the affected individuals cannot be readily identified or will not be able to be identified by the 10 day deadline, the PCLO will provide a generalized notice to the potentially impacted population by whatever means is most likely to reach the potentially affected individuals.

(4) If notification of affected individuals cannot be made within 10 working days, action will be initiated to notify the Deputy Secretary of Defense, per DoD 5400.11-R.

(5) If for good cause (e.g., law enforcement authorities request delayed notification to not jeopardize investigative efforts), notice can be delayed, but the delay will only be for a reasonable period of time. In determining what constitutes a reasonable period of delay, the potential harm to the individual must be weighed against the necessity for delayed notification.

(6) The notice to affected individuals will include at least the following information:

(a) The specific data involved. It is insufficient to simply state that personal information has been lost. Where names, SSNs, and dates of birth are involved, it is critical that the individual be advised that these data elements potentially have been compromised.

(b) The facts and circumstances surrounding the loss, theft, or compromise. The description of the loss should be sufficiently detailed so the individual can clearly understand how the compromise occurred.

(c) What protective actions DCMA is taking to mitigate against potential future harm.

(d) Reference to the Federal Trade Commission (FTC) public web site on identity theft. The site provides valuable information as to what steps individuals can take to protect themselves if their identities potentially have been or are stolen. The specific link to the FTC web site is listed on the resource page for this manual.

(e) A sample notification letter is on the resource page for this manual.

(7) The notification of affected individuals will be made regardless of whether the PII is contained in a system of records.

d. Actions Upon Discovery of an Incident.

(1) All incidents will be reported expeditiously. Quick reporting can prevent an incident from becoming a breach. The person discovering an incident will, at a minimum, report it to the PCLO and, if known, the Component Head/Capability Manager with cognizance over the information.

(2) The PCLO will maintain a record of all incidents, including the type of information listed in paragraph 4.4.b.(4). Incidents are not reported to DPCLTD or USCERT immediately, but the number of incidents is included on the Semi-Annual Component Privacy Report (see paragraph 7.1.).

(3) The applicable component officials will ensure the information exposed in the incident is either removed or becomes accessible to only those who are authorized to view the information as part of official duties. They will inform the PCLO when the action has been taken and provide details as needed for the PCLO's record of the incident.

SECTION 5: PRIVACY AND CIVIL LIBERTIES REQUESTS AND COMPLAINTS

5.1. PRIVACY ACT REQUESTS.

a. Individual Access to Personal Information. All individual requests must be in writing and must sufficiently describe the records being sought in order to identify the proper system of records and conduct a search with reasonable effort. If fees are applicable, the requester should include a statement regarding willingness to pay all fees (or those up to a specified amount), or request a waiver or reduction of fees. Individual access is intended for use by individuals who seek access to records about themselves that are maintained in a system of records. Release to someone of their own personal information is not considered public release of information.

b. Individual Requests for Access.

(1) Individuals must address requests for access to personal information in a system of records to the PCLO. See DoD 5400.11-R, subparagraph C3.1.10, for response time limitations.

(2) The individual is not required to explain or justify his or her need for access to his or her records. Before granting access to personal data, an individual may be required to provide reasonable proof of his or her identity. Procedure for verification of individual identity is documented in DoD 5400.11-R, subparagraph C3.1.3.

c. Personal Information Normally Considered Releasable. Personal information normally considered releasable is listed in DoD 5400.11-R, paragraph C4.2.2.5 and on the resource page for this manual.

d. Denial of Individual Access. An individual may be denied access to a record pertaining to him or her. The exemptions to release are listed in DoD 5400.11-R, paragraph C3.2 and on the resource page for this manual.

e. Exemptions. There are three types of exemptions permitted by the PA.

(1) Access Exemption. Records compiled in reasonable anticipation of a civil action or proceeding from the access provisions of the PA.

(2) General Exemptions. These exemptions are detailed in DoD 5400.11-R, paragraph C5.1.

(3) Specific Exemptions. These exemptions are detailed in DoD 5400.11-R, paragraph C5.1.

f. Denial Notifications. Formal denials of access must be in writing. The information required in the denial is listed in DoD 5400.11-R, subparagraph C3.2.3.

g. Fees. Assessing fees will be done in accordance with DoD Manual (DoDM) 5400.07, "DoD Freedom of Information Act (FOIA) Program," with the considerations set forth in DoD 5400.11-R, paragraph C3.4.

h. Amendment of Records. Individuals are allowed to review the personal information being maintained about them and to make requests to the applicable Component Head/Capability Manager if amendments are desired. This procedure is detailed in DoD 5400.11-R, paragraph C3.3.

i. Non-Agency Records. Certain documents under the physical control of DCMA used to assist DCMA in performing official functions are not considered "Agency records." These documents are identified in DoD 5400.11-R, subparagraph C3.1.8.

j. Relationship Between the PA and the FOIA. Requestors who seek records about themselves contained in a system of records will not be denied access to their personal information simply because they fail to cite or imply the proper act, PA, or FOIA. The Agency must make available to the requestor all of their own personal information contained in the system of records, except where access may be denied pursuant to an exemption claimed for the system.

5.2. PRIVACY COMPLAINT PROCEDURES. Any individual who believes their PII has been compromised should report the incident to the PCLO.

a. Means of Reporting. Privacy complaints are submitted by email to the DCMA Privacy Inbox using the email address listed on the resource page of this manual. The complaint will include:

(1) Employee's name.

(2) Employee's work address.

(3) Employee's work phone number.

(4) Employee's work email address.

(5) Date and location of the alleged violation.

(6) Whether the violation is ongoing.

(7) Any additional information the employee can provide to help the Agency investigate the complaint.

b. Complaint Investigation. The PCLO will, in conjunction with applicable Component Head/Capability Manager(s) and others as necessary, conduct a thorough investigation into the complaint. The investigation process includes an initial assessment of the complaint to determine whether it comprises a breach, an incident, or is not a violation of the PA.

(1) If a breach has occurred, the reporting procedures described in paragraph 4.4. apply.

(2) If an incident has occurred, the PCLO will:

(a) Notify the SCOP.

(b) Notify the owner of the information or document to have the material removed or destroyed immediately. If the owner cannot be identified within two (2) business days, the PCLO will notify the applicable Component Head/Capability Manager(s) to have the material removed or destroyed immediately.

(c) Keep a record of the incident for reporting purposes. The record will include the following information:

1. Date and time of incident.

2. Type of record.

3. Record owner.

4. Disposition of the incident.

5. Date the incident was closed.

5.3. CIVIL LIBERTIES COMPLAINT PROCEDURES.

a. Means of Reporting. Civil liberties complaints are submitted by email to the DCMA Civil Liberties Inbox using the email address listed on the resource page for this manual. The complaint should include:

(1) Employee's name.

(2) Employee's work address.

(3) Employee's work phone number.

(4) Employee's work email address.

(5) Date and location of the alleged violation.

(6) Whether the violation is ongoing.

(7) Which civil rights the employee believes was violated.

(8) Any additional information the employee can provide to help the Agency investigate the complaint.

b. Complaint Investigation. The PCLO, in conjunction with the appropriate representatives from DCMA Components, Capabilities, and/or others as necessary, will conduct a thorough investigation into the complaint. The first step of the investigation process includes an initial assessment of whether the matter may actually be a violation of civil liberties. This step obviates the need for further investigation in case the complainant does not fully understand what constitutes a violation.

(1) If the complaint does not identify a violation of civil liberties, the PCLO will notify the complainant in writing and explain why the matter being reported is not a violation.

(2) If the PCLO's initial assessment is that the matter is or may be a violation, the PCLO, in conjunction with the appropriate representatives from DCMA Components, Capabilities, and/or others as necessary, will:

(a) Continue researching the circumstances of the violation.

(b) Develop a resolution plan.

(c) Implement the resolution plan.

(d) Respond to the complainant.

(e) Report completion of the matter to the SCOP, CIO, and other DCMA officials as required.

(f). Report close out of the matter to DPCLDT via the means established by DPCLDT, which is listed on the resource page for this manual.

5.4. APPEAL OF PRIVACY AND CIVIL LIBERTIES COMPLAINT RESOLUTIONS.

a. If a complainant is not satisfied with the PCLO's decision on resolution of the complaint, they may appeal to the SCOP, citing the reasons for their disagreement with the PCLO's decision.

b. If a complainant is not satisfied with the SCOP's decision on resolution of the complaint, they may appeal to the DCMA Deputy Director, citing the reasons for their disagreement with the SCOP's decision.

c. If a complainant is not satisfied with the Deputy Director's decision on resolution of the complaint, they may appeal to the DCMA Director, citing the reasons for their disagreement with the Deputy Director's decision. The Director's decision will represent the Agency's final decision on resolution of the complaint.

SECTION 6: PRIVACY ACT REMEDIES AND PENALTIES

6.1. ADMINISTRATIVE REMEDIES. Any individual who believes he or she has a legitimate complaint or grievance against DCMA, any DCMA or DoD employee, or the DoD concerning any right granted by the PA must be permitted to seek relief through appropriate administrative channels without reprisal. Questions can be forwarded to the PCLO via the DCMA Privacy Inbox. The email address is on the resource page for this manual.

6.2. CIVIL ACTIONS. An individual may file a civil suit against any DoD Component, as documented in DoD 5400.11-R, paragraph C10.2.

6.3. CIVIL REMEDIES. Civil remedies are documented in DoD 5400.11-R, paragraph C10.3. While civil penalties are imposed on agencies, employees responsible for civil violations for which the Agency has been penalized are subject to administrative sanctions, such as removal from employment.

6.4. CRIMINAL PENALTIES. Criminal penalties are documented in DoD 5400.11-R, paragraph C10.4.

6.5. LITIGATION STATUS SHEET. Whenever a complaint citing the PA is filed in a U.S. District Court against DCMA or a DCMA employee, the responsible Component Head/ Capability Manager must notify the PCLO, who will review and forward to the DCMA GC and the DPCLTD. The litigation status sheet, provided as Appendix 8 of DoD 5400.11-R, provides a standard format for this notification. The initial litigation status sheet forwarded must, as a minimum, provide the information required by items 1 through 6. A revised litigation status sheet must be provided at each stage of the litigation. When a court renders a formal opinion or judgment, copies of the judgment and opinion must be provided to the PCLO and an update will be provided to the DPCLTD with the litigation status sheet reporting that judgment or opinion.

SECTION 7: REPORTING REQUIREMENTS

7.1. SEMI-ANNUAL COMPONENT PRIVACY REPORT. This process is documented in OMB Circular A-130. The most recent format for the report is on the resource page for this manual.

7.2. FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) REPORT. This report is combined by DPCLTD with those from other DoD agencies and sent to Congress to ensure consistent government-wide performance and best practices to protect national security, privacy, and civil liberties while limiting the economic and mission impact of incidents. The most recent format for the report is on the resource page for this manual.

7.3. SEMI-ANNUAL CIVIL LIBERTIES REPORT. This report is combined by DPCLTD with other DoD agencies and sent to Congress and the Privacy and Civil Liberties Oversight Board in order to inform Congress of the discharge of each of the functions of the Civil Liberties offices concerned. This report is in accordance with Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, Section 2000ee-1 of Title 42 U.S.C. The most recent format for the report is on the resource page for this manual.

SECTION 8: TRAINING REQUIREMENTS

8.1. DCMA PERSONNEL. All DCMA personnel are required to complete training on the PA and the safeguarding of PII. New employees will receive the initial training at orientation; after which it will be completed on an annual basis.

8.2. ROLE-BASED TRAINING REQUIREMENTS. DCMA personnel who perform in special roles specific to privacy and civil liberties will receive training in addition to the requirements listed in paragraph 8.1. The training requirements for these personnel are listed on the resource page for this manual. Examples of these special roles are:

a. SCOP and PCLO. The persons in these positions have a primary responsibility for implementing the DCMA Privacy and Civil Liberties program.

b. Persons involved in the design, development, operation, and maintenance of any system of records. The PA requires government agencies to establish rules of conduct for all persons involved in the design, development, operation, and maintenance of any system of records and to train these persons with respect to these rules. The DCMA Rules of Conduct are contained in paragraph 3.5. of this manual.

c. Persons whose responsibilities require greater access than normal in the performance of their duties. Examples of personnel in this category are supervisors, data systems administrators, performance assessment administrators, human resources specialists, job interview panelists, and public affairs specialists.

8.3. DCMA CONTRACTORS. FAR Subpart 24.3 details contractor requirements for the protection of privacy and for privacy training. This includes a required clause (FAR 52.224-3) in solicitations and contracts when, on behalf of the Agency, contractor employees will do any of the following:

a. Have access to a system of records.

b. Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle PII.

c. Design, develop, maintain, or operate a system of records.

GLOSSARY

G.1. DEFINITIONS.

Breach. An occurrence in which information has been compromised or disclosed or acquired without authorization, and the Agency has lost control over the use of the information, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII; or (2) an authorized user accesses PII for an other than authorized purpose.

Civil Liberties. Fundamental rights and freedoms protected by the Constitution of the United States.

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, government agency, or private entity other than the subject of the record, the subject's designated agent, or the subject's legal guardian.

FISMA. U.S. legislation defining a comprehensive framework to protect government information, operations, and assets against natural or man-made threats.

Incident. An occurrence in which information, usage of which is still under the control of the Agency, actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Individual Access. Access to information pertaining to the individual by the individual or his or her designated agent or legal guardian.

Lost, Stolen, or Compromised Information. See Breach.

Need to Know. A determination that a prospective recipient requires access to specific information in order to perform or assist in a lawful and authorized governmental function.

PA Request. A request from an individual for notification as to the existence of access to, or amendment of records pertaining to that individual. These records must be maintained in a system of records.

PAS. Information on a form being used to collect personal information from an individual or on a separate form that can be retained by that individual describing (a) the authority which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary; (b) the principal purpose or purposes for which the information is intended to be used; and (c) the routine uses which may be made of the information; and (d) the effects on that person, if any, of not providing all or any part of the requested information.

PCLO. The DCMA employee who is responsible for the day-to-day management of the Privacy and Civil Liberties program.

PII. Information about an individual that identifies, links, relates, or is unique to, or describes him or her; e.g., an SSN, age, military rank, civilian grade, marital status, race, salary, home/office phone numbers, other demographic, biometric, personnel, medical, and financial information.

Record. Any item, collection, or grouping of information, whatever the storage media (paper, electronic, etc.), about an individual that is maintained by a DoD Component, including, but not limited to, an individual's education, financial transactions, medical history, criminal or employment history, and that contains his or her name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print, or a photograph. To be considered a record under DCMA's release cognizance, (1) DCMA must have expressly created or obtained the record for exclusive use from another entity; and (2) the record was under DCMA's control. The control elements include an examination of (a) DCMA's ability to retain or relinquish control; (b) the creator's intent; and (c) the extent to which DCMA relies upon the document.

Risk Assessment. An analysis considering information sensitivity, vulnerabilities, and cost in safeguarding personal information processed or stored in DCMA.

SAOP. The official designated by the head of a federal agency, such as DoD, as the person responsible for the privacy and civil liberties programs throughout that agency.

SCOP. The DCMA general/flag officer, Senior Executive Service member, or senior level employee responsible for the overall implementation of the Privacy and Civil Liberties program.

System of Records. A group of records under the control of an agency from which information is retrieved by the name of an individual, or by any number, symbol, or other unique identifier assigned to that individual.

SORN. A notice published by an agency in the FR upon the establishment and/or modification of a system of records describing the existence and character of the system. A SORN identifies the system of records, the purpose(s) of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom records are maintained, the routine uses to which the records are subject, and additional details about the system, as desired.

Violation of Civil Liberties. Unlawful government interference with the exercise of fundamental rights and freedoms protected by the Constitution of the United States.

GLOSSARY

G.2. ACRONYMS.

CIO	Chief Information Officer
DC	DCMA Corporate Operations
DCC	DCMA Strategic Communication
DD Form 2923	Privacy Act Data Cover Sheet
DoDD	DoD Directive
DoDI	DoD Instruction
DoDM	DoD Manual
DPCLTD	Defense Privacy, Civil Liberties, and Transparency Division
EEO	Equal Employment Opportunity
FAR	Federal Acquisition Regulation
FIPPS	Fair Information Practice Principles
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FR	Federal Register
FTC	Federal Trade Commission
GC	General Counsel
IT	Information Technology
OMB	Office of Management and Budget
PA	Privacy Act
PAS	Privacy Act Statement
PCLO	Privacy and Civil Liberties Officer
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
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
USCERT	U.S. Computer Emergency Readiness Team

REFERENCES

Administrative Instruction 102, "Office of the Secretary of Defense (OSD) Federal Register (FR) System," November 6, 2006, as amended
DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
DoD Directive 5105.64, "Defense Contract Management Agency (DCMA)," January 10, 2013
DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014
DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," July 14, 2015, as amended
DoD Instruction 8580.02, "Security of Individually Identifiable Health Information in DoD Health Care Programs," August 12, 2015
DoD Manual 5400.07, "DoD Freedom of Information Act (FOIA) Program," January 25, 2017
Federal Acquisition Regulation, Subpart 24.1, "Protection of Individual Privacy"
Federal Acquisition Regulation, Subpart 24.3, "Privacy Training"
Federal Acquisition Regulation, Clause 52.224-3
Office of the Deputy Chief Management Officer Memorandum, "Designation of Senior Component Officials for Privacy and Establishment of Roles and Responsibilities," August 28, 2017
Office of Management and Budget Circular No. A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication Under the Privacy Act," December 12, 2016
Office of Management and Budget Circular No. A-130, "Managing Information as a Strategic Resource," July 28, 2016
United States Code, Title 5, Section 552 (also known as "The Freedom of Information Act (FOIA)")
United States Code, Title 5, Section 552a (also known as the "Privacy Act," as amended)
United States Code, Title 42, Sections 2000ee and 2000ee-1
United States Code, Title 44, Section 3303a