DEPARTMENT OF DEFENSE
Defense Commissary Agency
Fort Lee, VA 23801-1800

MANUAL

Privacy Act Program Manual

DeCAM 80-21.1
May 18, 2010

General Counsel
OPR: DeCA/GC

1. POLICY. This Manual:

a. Reissues Defense Commissary Agency Manual (DeCAM) 80-21.1 (Reference (a)).

b. Is issued under the authority of DeCA Directive (DeCAD) 80-21 (Reference (b)).

c. Is established in compliance with references listed herein.

2. PURPOSE. This Manual provides procedures for carrying out the policy, assigns responsibilities, and provides guidance and procedures to enable DeCA employees to comply with the Privacy Act of 1974 (Reference (c)), in accordance with provisions of Department of Defense (DoD) Directive 5400.11 (Reference (d)).

3. APPLICABILITY. This Manual applies to all DeCA activities and all DeCA personnel.

4. MANAGEMENT CONTROL SYSTEM. This Manual contains internal management control provisions that are subject to evaluation, testing, and other requirements of DeCAD 70-2 (Reference (e)) and as specified by the Federal Managers' Financial Integrity Act.

5. RELEASABILITY – UNLIMITED. This Manual is approved for public release and is located on DeCA's Internet Web site at www.commissaries.com.

6. EFFECTIVE DATE. This Manual is effective immediately.

William E. Sherman
General Counsel

TABLE OF CONTENTS

Chapter 6 – Privacy Impact Assessments (PIA)

Chapter 7 – Privacy Act Statements

Chapter 8 – Breach Procedures

Chapter 9 – Penalties for Noncompliance

Chapter 10 – Access by Individuals

APPENDICES

GLOSSARY

REFERENCES

(a) DeCA Manual 80-21.1, "Privacy Act Program Manual," July 2, 2009 (hereby canceled)
(b) DeCA Directive 80-21, "Privacy Act Program," April 15, 2010
(c) Section 552a of Title 5, United States Code, "The Privacy Act of 1974," as amended
(d) DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007
(e) DeCA Directive 70-2, "Internal Control Program," December 17, 2007
(f) Office of Management and Budget Circular No. A-130, Appendix I, "Federal Agency Responsibilities for Maintaining Records About Individuals"
(g) Public Law 107-347, 116 Stat. 2899, "E-Government Act of 2002," December 17, 2002
(h) Executive Order 9397, "Numbering System for Federal Accounts Relating to Individual Persons," November 22, 1943
(i) OSD Policy Memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)," June 5, 2009
(j) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
(k) DoD Directive 5400.07, "DoD Freedom of Information Act (FOIA) Program," January 2, 2008
(l) DoD 5400.7-R, "DoD Freedom of Information Act Program," September 4, 1998
(m) DeCA Directive 30-12, "Freedom of Information Act (FOIA) Program," January 27, 1995
(n) DoD 5200.1-R , "Information Security Program", January 1997
(o) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
(p) DeCA Directive 30-18, "Defense Commissary Agency Security Programs," March 1, 1997
(q) DoD Directive 5105.55, "Defense Commissary Agency (DeCA)," March 12, 2008

CHAPTER 1

INTRODUCTION

1-1. PURPOSE. This Manual has been developed to provide all DeCA employees and contractors with program reference and direction for complying with the Privacy Act of 1974 (Reference (c)). The guidance contained herein applies to all DeCA activities and all DeCA personnel. All references to Privacy contained throughout this Manual pertain to Reference (c). For purposes of this Manual, "DeCA personnel" includes contractors who must use, have access to, or disseminate individually identifiable information subject to the Privacy Act in order to perform their duties.

1-2. BACKGROUND. The development and maintenance of this Manual is supported by Reference (d) and is to be used in coordination with DoD directives, regulations, and supporting guidance listed in References.

1-3. PRIVACY ACT PROGRAM MISSION. The primary mission of the DeCA Privacy Act Program is to ensure that personal information is collected, maintained, used, or disclosed in accordance with Reference (c). Additionally, DeCA employees have a continuing affirmative responsibility to safeguard personally identifiable information (PII) in its possession and to prevent its theft, loss, or compromise. The DeCA Privacy Office exists to support DeCA in meeting its responsibilities in delivering the commissary benefit to Service members and to help improve DeCA's performance and accountability in complying with statutory regulations.

1-4. FEEDBACK. The Privacy Office General Counsel (GC) is receptive to suggestions for improving this Manual and recommendations can be sent to the Defense Commissary Agency, Attn: Privacy Office GC, 1300 E Avenue, Fort Lee, VA 23801-1800, telephone (804) 734-8000 Extension 48116 (DSN 687), or via e-mail to GeneralCounsel@deca.mil. Any questions pertaining to this Manual should be directed to the Privacy Officer (GC).

CHAPTER 2

RESPONSIBILITIES

2-1. DIRECTOR OF DeCA/CHIEF EXECUTIVE OFFICER (CEO). The Director/CEO is responsible for overseeing the administration of the DeCA Privacy Program.

2-2. CHIEF OF STAFF (COS). The appellate authority for Privacy Act requests resides with the COS.

2-3. SENIOR PRIVACY OFFICIAL (SPO). The General Counsel serves as the SPO. The SPO administers the operations of the DeCA Privacy Office and provides policy guidance. The SPO is the DeCA Denial Authority.

2-4. DEPUTY GENERAL COUNSEL (DGC), LITIGATION/FREEDOM OF INFORMATION ACT (FOIA). The DGC for the Privacy Program shall:

a. Provide supervisory guidance to the Privacy Officer.

b. Provide advice and assistance on all legal matters arising out of, or incident to, the administration of the DeCA Privacy Program.

c. Ensure all aspects of the Privacy Program are fully implemented.

2-5. PRIVACY OFFICER (PO). The PO shall:

a. Manage the Privacy Act Program for DeCA.

b. Provide guidance, assistance, and training to Agency personnel.

c. Control and monitor Privacy Act requests received and coordinate with the office(s) of primary responsibility for response.

d. Prepare and submit System of Records Notices (SORN) to the Defense Privacy Office for publication in the Federal Register.

e. Coordinate with the Office of the Chief Information Officer on overarching policy implementation.

f. Receive, evaluate, and, where appropriate, report suspected or substantiated breaches of Privacy protected information.

2-6. REGION DIRECTOR, FUNCTIONAL PROCESS OWNERS/SPECIAL STAFF GROUP (FPO/SSG). Each region director and FPO/SSG shall:

a. Appoint a Privacy point of contact (POC) who will serve as the principal on Privacy matters and

maintain suspense control of Privacy actions, providing responsive documents to the FOIA/PO.

b. Take appropriate remedial action upon being advised of a substantiated Privacy Act violation or known or suspected breaches of Privacy protected information.

2-7. SUPERVISORS. All supervisors shall:

a. Ensure all DeCA employees and contractors receive mandatory initial Privacy Act training and annual refresher training thereafter.

b. Ensure actual or suspected breaches of Privacy protected information are immediately reported to the PO.

2-8. SYSTEM MANAGER (SM). Any individual having authority for maintaining a group of records containing personal information is referred to as the SM. The SM is responsible for ensuring that a government-wide SORN covers the system of records and, if not, preparing and submitting a DeCA-specific SORN to the PO.

2-9. DeCA EMPLOYEES AND CONTRACTORS. All Agency employees/contractors must ensure strict adherence to the safeguarding of Privacy protected data at all times and report any known or suspected breaches.

CHAPTER 3

HANDLING/SAFEGUARDING PRIVACY ACT DATA

3-1. GENERAL. In order to ensure that the Privacy Act policies and procedures are followed, all DeCA personnel must adhere to appropriate administrative precautions and physical safeguarding methods. The information technology (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 consistent with DoD and Agency requirements, as listed in References.

3-2. COLLECTING PRIVACY ACT 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. It may not be practical to collect personal information directly from an individual in all cases. Some examples are:

a. Verification of information through third party sources for security or employment suitability determinations.

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

c. When obtaining the needed information directly from the individual is exceptionally difficult or may result in unreasonable costs.

d. 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.

3-3. STORING PRIVACY DATA. 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 access/enter the work space. Computers should be locked when leaving a workstation.

a. Passwords should be safeguarded at all times.

b. After duty hours, if the building is locked or manned by security, records containing PII should be placed in closed drawers or cabinets.

c. Special categories of Privacy data (i.e., medical files, investigative files, adverse action files) should be placed in LOCKED offices, drawers, or cabinets.

d. Refer to paragraph 3-6 for guidelines pertaining to storage of PII while on temporary duty (TDY).

e. Prior to collecting and/or maintaining PII, refer to:

(1) System Notice requirements defined in Chapter 5

(2) Privacy Act Statement guidelines defined in Chapter 7.

3-4. SHARING/HANDLING PRIVACY DATA. Always follow the "need-to-know" principle.

a. Follow these guidelines:

(1) Prior to sending an e-mail with "reply to all" or when sending mass mailings, ensure that all recipients actually have a need for the information.

(2) Prior to sending a document to an unsecured facsimile (fax) machine, call the intended recipient to ensure prompt pickup.

(3) Be mindful not to leave documents unattended at the copier or fax machine.

(4) Exercise caution when printing; make certain the correct printer is selected and ensure prompt retrieval.

b. Sharing Privacy Data Within DeCA. Share only with those specific DeCA personnel who need the data to perform official, assigned duties.

c. Sharing Privacy Data Within the DoD. Information may also be shared with DoD employees/ contractors who need the data to perform official, assigned duties. However, a written request (on Agency/Component letterhead and signed by an authorized official) should be obtained prior to release of such information.

d. Sharing Privacy Data Outside of DeCA and DoD. Share only with those individuals and entities that are listed in the routine use and disclosure clause of the governing Privacy Act SORN. If uncertain which SORN governs the system of records, contact the privacy officer for assistance. A written request (on letterhead and signed by an authorized official) should be obtained prior to release of such information.

NOTE: If one has doubts about sharing data, consult with the supervisor or privacy officer.

3-5. REMOVING PRIVACY DATA. Privacy data must never be removed from the work location UNLESS it is required in the performance of official duties.

a. Written consent from the immediate supervisor MUST be obtained and must identify the following:

(1) Type/description of data.

(2) Reason for removal.

(3) Date and expected time for return.

b. Questions or concerns about whether it is appropriate to grant authority may be addressed to the privacy officer, Deputy General Counsel Litigation/FOIA, or SPO, all located in GC.

c. When TDY, ensure that records are secured in the local DeCA facility OR secure them out of sight in the hotel or billeting facilities.

d. When teleworking, treat Privacy protected data as if it was their own most sensitive personal/ financial information.

3-6. TRANSMITTING PRIVACY DATA. Ensure that appropriate steps, such as those outlined below, are taken when transmitting Privacy protected data.

a. When transmitting Privacy data by postal or commercial shipping:

(1) Use double-wrap, using an inner and outer envelope, if appropriate. (For example, use an inner and outer envelope when sending a package addressed to the store, but to the attention of an employee.)

(2) Mark on the inner envelope that it contains Privacy Act data.

(3) Mark the outer envelope to the attention of an authorized recipient.

(4) Never indicate on the outer envelope that the contents contain Privacy data.

b. When hand-carrying Privacy data, ensure the following:

(1) Contents are shielded from view by using envelopes. As appropriate, use a DeCA Form 30-34, Sensitive Unclassified Information cover sheet or DD Form 2923, Privacy Act Data Cover Sheet.

(2) Never use interoffice envelopes (“holey joes”) or messenger-type envelopes unless the material is placed in an inner, sealed envelope.

c. When e-mailing personal information:

(1) State that the e-mail contains Privacy protected information in the opening line and in the last line of text.

(2) Never “Reply to All” when an e-mail contains an attachment with Privacy protected information unless there is an official need for all addressees to receive the information.

(3) Exercise caution when attaching documents containing PII to ensure that unnecessary information is removed.

(4) Encrypt all e-mail containing PII, privileged, confidential agency, or commercial information.

d. When sending personal information by fax:

(1) Use a fax cover sheet.

(2) Make sure the cover sheet clearly indicates the recipient and that the fax contains Privacy Act data.

(3) If the receiving fax machine is in a common area (i.e., if it is uncertain whether the fax is in a secured area), call ahead to make arrangements for receipt.

3-7. DISPOSAL OF PRIVACY DATA. When no longer required, Privacy Act data should be disposed of in a manner that renders the information unrecognizable or beyond reconstruction. Use any means that prevents/accomplishes the task and prevents inadvertent compromise.

a. Refer to the Agency Records Schedule or General Records Schedule (GRS) for proper disposition of Agency records.

b. Questions regarding appropriate disposal methods should be addressed to the Agency Records Office.

CHAPTER 4

TRAINING

4-1. PURPOSE. The purpose of the DeCA Privacy training program is to establish cultural awareness of and sensitivity to the protection of personal information pertaining to individuals, as well as to provide the knowledge concerning Privacy Act issues to ensure Agency compliance with Reference (c). Training includes the following:

a. Information regarding Privacy laws, regulations, policies and procedures governing DeCA's collection, maintenance, use, or dissemination of personal information.

b. Guidelines for all persons who use or are involved in the design, development, operation, and maintenance of any system of records.

c. Reminders that all DeCA personnel are responsible for safeguarding PII.

d. Penalties for noncompliance.

4-2. PRIVACY AWARENESS. It is to be understood that, where PII is involved, DeCA personnel should handle and treat the information as if it was their own information. Privacy Awareness flyers/slides are to be posted throughout DeCA facilities to further stress employees' responsibilities and advise individuals of their rights under the Privacy Act. Slides are located in Public Folders, General Counsel (GC), FOIA/Privacy Act Guidance.

4-3. TRAINING. All DeCA employees and contractor personnel as described in paragraph 1-1 must complete mandatory Agency Privacy Act Awareness Training initially as orientation and on an annual basis. This training provides a basic understanding of the Privacy Act as it applies to the individual's roles and responsibilities. In addition, employees with specific responsibilities under the Privacy Act must have a thorough understanding of the requirements outlined in this Manual. The Privacy Act Awareness Training slides are located on DeCA's Web site www.commissaries.com/employees/careers_and_training/center_for_learning/mandatory_training/.

a. This training is a prerequisite to obtaining access to DoD systems.

b. Annual refresher training must be provided to ensure that DeCA personnel understand their responsibilities.

c. The Certificate of Completion shall be executed at the completion of orientation and annual refresher training.

d. The Certificate of Completion shall be retained in the employee file or such other place as designated.

e. The certifications are subject to inspection during reviews by the Agency Inspector General and/or Agency privacy officials.

CHAPTER 5

SYSTEM OF RECORDS NOTICE (SORN) REQUIREMENTS

5-1. PURPOSE. The Privacy Act provides that the Government shall ensure that each newly proposed system of records is evaluated for need and relevancy and inform people at the time it is collecting information about them, why this information is being collected, and how it will be used. This is accomplished by the publication of a SORN, also referred to as a System Notice, in the Federal Register that fully describes the system. This description includes the data elements collected, where the records are located, how long they will be kept, how they will be used, and similar details. A system of records is a group of files that:

a. Contain an individual's name, Social Security number (SSN), or some other unique personal identifier (such as employee number) and at least one other element of personal information about the individual (such as date of birth). The system need only contain one actual personal identifier (i.e., an SSN, a name) that is tied to some other type of information about that person.

b. Are retrieved by an individual's name, SSN, or personal identifier and must actually retrieve information by personal identifier (i.e., the system is designed to retrieve information as a matter of practice); not merely the capability of retrieval.

5-2. SYSTEM MANAGER (SM) RESPONSIBILITIES. The individual responsible for maintaining the group of records containing personal information is referred to as a system manager (SM), whether it be a paper file system of records or an electronic system of records. It is the responsibility of the SM to ensure that there is a need and relevancy to collect Privacy data. The SORN requirements pertain to any collection of personal information, to include paper file systems as well as records maintained in an IT system. In addition to ensuring a SORN covers their system of records, each Agency SM has specific responsibilities for their system of records, as follows:

a. Identify the required controls and individuals authorized access to personal information and maintaining updates to the access authorizations.

b. 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 Reference (b).

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

d. If records are disclosed (outside of DoD or under the FOIA) without the consent of the record subject, a record of disclosure must be maintained.

e. Conduct reviews in accordance with Appendix I to the Office of Management and Budget (OMB) Circular A-130 (Reference (f).

f. Ensure records are kept in accordance with retention and disposal requirements set forth in the Agency Records Schedule and/or the GRS.

5-3. EVALUATION OF PROPOSED SYSTEM OF RECORDS. Each new proposed system of records must be evaluated during the planning stage. The following factors should be considered:

a. Relationship of data to be collected and retained to the purpose for which the system is maintained. All information must be relevant to the purpose; i.e., each element of data being collected must have a purpose and a specific intended use.

b. The impact on the purpose or mission if categories of information are not collected. All data fields must be relevant and necessary to accomplish a lawful purpose or mission.

c. The disposition schedule.

d. The method of disposal.

e. Cost of maintaining the information.

5-4. PREPARATION OF SYSTEM NOTICE. The following steps are intended to provide assistance in determining if an existing Notice may cover the proposed system of records, or if a new SORN must be developed.

a. Prior to collecting Privacy data, the SM must either:

(1) Confirm that an existing government-wide SORN fully covers the proposed collection refer to DoD Web site http://www.defenselink.mil/privacy/govwide/ for the list of government-wide SORNs); or,

(2) Prepare an Agency SORN, in coordination with the Agency Privacy Officer.

b. If a government-wide SORN exists that appropriately covers the records in the system of records, the SM may use the existing SORN. Ensure that the collection purposes, methods, uses, etc., are <u>all</u> consistent with the government-wide SORN and that there are no DeCA-specifics falling outside of that SORN.

c. If no existing government-wide SORN exists that is relevant to the system of records, the SM must prepare and submit to the Privacy Officer a draft SORN. See the Privacy Officer:

(1) To verify that an existing government-wide Notice does not exist.

(2) For assistance in developing and maintaining a DeCA-specific SORN.

d. The Privacy Officer will:

(1) Provide an easy-to-use template which consists of several documents:

(a) Narrative Statement.

(b) Notice (to the Office of Secretary of Defense) to Add a New System of Records.

(c) SORN.

(2) Once the documents have been finalized, submit the package to the Defense Privacy Office for coordination and final approval.

(3) Upon approval by the Defense Privacy Office, the Notice is submitted to the Federal Register for a 30-day Public Comment Notice.

(4) Once final comments are received and adjudicated, the Notice is published in the Federal Register.

e. Prior to altering (paragraph 5-5) or revising any existing record system, the system must first be reviewed and evaluated (paragraph 5-3) to determine if the SORN must also be revised.

5-5. ALTERED RECORDS SYSTEMS. A system is considered altered whenever one of the following actions occurs or is proposed:

a. A significant increase or change in the number, type, or category of individuals about whom records are maintained.

(1) Increases in numbers of individuals due to normal growth are not considered alterations unless they alter the character and purpose of the system.

(2) Increases that significantly change the scope of population covered.

b. An expansion in the types or categories of information maintained.

c. A change in the purpose for which the information in the system is used. The new purpose must not be compatible with the existing purpose(s) for which the system is maintained. If the use is compatible and reasonably expected, there is no change in purpose and no alteration occurs.

d. A change to equipment configuration (either hardware or software) that creates substantially greater or easier access to the records in the system of records.

(1) Increasing the number of offices with direct access is an alteration.

(2) Software applications such as operating systems and system utilities which provide for easier access are considered alterations.

(3) Changes to existing equipment configuration with on-line capability need not be considered alterations to the system if the change does not alter the present security posture.

e. The addition of an exemption pursuant to Section (j) or (k) of Reference (c).

f. The addition of a routine use pursuant to paragraph (b)(3) of Reference (c).

5-6. PENALTIES FOR NONCOMPLIANCE. It is illegal to maintain a system of records without having an approved Systems Notice published in the Federal Register. The Privacy Act imposes criminal penalties **directly on the individual** for violations of certain provisions of the Act. Refer to Chapter 9 for details.

CHAPTER 6

PRIVACY IMPACT ASSESSMENTS (PIA)

6-1. PURPOSE. Section 8 of the E-Government Act of 2002 (Reference (g)) establishes requirements for conducting, reviewing, and publishing privacy impact assessments (PIA) when purchasing or creating new IT systems or when initiating new electronic collections of information in identifiable form. A PIA addresses privacy factors for all new or significantly altered IT systems or projects that collect, maintain, or disseminate personal information pertaining to individuals.

6-2. OFFICE OF RESPONSIBILITY. The office of primary responsibility for PIAs is the Chief Information Officer.

CHAPTER 7

PRIVACY ACT STATEMENTS

7-1. PURPOSE. When an individual is requested to furnish personal information that will be included in a system of records, a Privacy Act Statement is required regardless of the collection medium (paper or electronic forms, personal interviews, telephonic interviews, or other methods). The statement informs individuals why the information is being collected and how it will be used. It also enables the individual to make an informed decision whether to provide the information requested. If the personal information solicited is not to be incorporated into a system of records, the statement is not required. However, personal information obtained without a Privacy Act Statement shall not be incorporated into any system of records.

7-2. HOW TO PREPARE A PRIVACY ACT STATEMENT.

a. A Privacy Act Statement must include the following four elements:

(1) Authority. A Federal statute or Executive Order of the President must authorize the collection and maintenance of a system of records. Whenever possible, cite the specific provisions of the statute or Executive Order. When using general statutory grants of authority as the primary authority, the regulation/directive/instruction implementing the statute within DeCA should also be identified. Executive Order 9397 (Reference (h)) authorizes solicitation and use of SSNs as numerical identifiers for individuals in most Federal record systems; however, it does not provide mandatory authority for soliciting. When collecting the SSN, always place 'E.O. 9397 (SSN)' in the authority; however, note that this Executive Order will never stand alone as an authority to collect and maintain information under the Privacy Act.

Example: "Authority. 42 U.S.C. 2000e-16(b) and (c); 29 U.S.C. 204(f) and 206(d); Exec. Order No. 12106, 44 FR 1053 (Jan. 3, 1979)"

(2) Purpose. State the primary purpose for the collection.

Example: "Purpose. These records are maintained for the purpose of counseling, investigating, and adjudicating complaints of employment discrimination brought by applicants and current and former federal employees against federal employers."

(3) Disclosure. Describe whether mandatory or voluntary; include the result of failure to provide the information.

Example: "Disclosure. Providing this information is voluntary; however, if you do not provide this information, you may not be eligible to receive benefits."

(4) Routine Uses. Summarize the uses contained in the SORN that covers the specific system of records; specifically, the paragraph entitled "Routine uses of records maintained in the system, including categories of users and the purposes of such uses."

Example: "Routine Uses. The information on this form may be used (a) in the counseling of an informal complaint of discrimination; (b) in the processing and adjudication of the complaint and any appeal concerning the complaint; and (c) as a data source for production of summary descriptive statistics and analytical studies of complaint processing and resolution efforts."

b. Contact the Agency Privacy Officer if assistance is needed in the preparation of a Privacy Act Statement.

CHAPTER 8

BREACH PROCEDURES

8-1. PURPOSE. Reporting of any breach (or potential breach) of personal information is required when there is a loss, theft, or compromise of PII. A breach is defined as a "loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic." This section is intended to provide DeCA personnel with breach reporting guidelines; to assist in determining the risk of harm when a breach or potential compromise involving PII occurs; and to improve the decision making process relative to breach notification and reporting. Breaches subject to reporting and notification include both electronic systems and paper documents. (Refer to Reference (i)).

8-2. REPORTING INAPPROPRIATE DISCLOSURES. Once a loss, theft, or compromise of information has been discovered, the breach shall immediately be reported as follows:

a. Reporting Organization/Activity.

(1) Without delay, contact the Privacy Office in GC to report a suspected Privacy breach. Identify as much information as possible, to include:

(a) The organization/activity involved.

(b) The date of the breach.

(c) The date of the discovery of the breach.

(d) If known, specify the number of individuals impacted.

(e) Describe the facts and circumstances surrounding the loss, theft, or compromise.

(f) Describe the actions taken in response to the breach.

(2) Follow-up the phone call with a written description of the incident, providing a thorough accounting of the event/incident. E-mail the documentation to the Privacy Officer, including copies of any backup documentation. If it is not possible to send the information via e-mail, fax the information to (804) 734-8259.

(3) If a breach involves government-authorized credit cards, the issuing bank must be notified.

b. Privacy Office. The SPO or designee shall:

(1) Notify the United States Computer Emergency Readiness Team (U.S. CERT) within 1 hour of discovering that a reportable breach of PII has occurred.

(2) Notify the Director of DeCA and the Defense Privacy Office (concurrently) of the breach within 48 hours upon being notified that a loss, theft, or compromise has occurred. The notification shall be in writing and should be concise, conspicuous, and in plain language, and shall include the following elements:

(a) Identify the organization involved.

(b) Specify the date of the breach.

(c) Specify the date of the discovery of the breach.

(d) Specify the number of individuals impacted to include whether they are DeCA civilian, military, or contractor personnel; DeCA civilian or military retirees; family members; other Federal personnel or members of the public, etc.

(e) Briefly describe the facts and circumstances surrounding the loss, theft, or compromise.

(f) Briefly describe actions taken in response to the breach, to include:

1 Whether the incident was investigated and by whom.

2 The preliminary results of the inquiry, if then known.

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

4 Whether the affected individuals are being notified and if this will not be accomplished within 10 working days, that action will be initiated to notify the Deputy Secretary of Defense.

5 What remedial actions have been, or will be, taken to prevent a similar such incident in the future; e.g., refresher training conducted, new or revised guidance issued.

6 Any other information considered pertinent as to actions to be taken to ensure that information is properly safeguarded.

(3) Notify the region director/FPO/SSG Privacy POC as soon as possible after other required notifications have been accomplished.

8-3. RISK ANALYSIS TO DETERMINE IF IMPACTED INDIVIDUAL(S) SHOULD BE NOTIFIED.

a. Notification of a breach when there is little or no risk of harm might create unnecessary concern and confusion. Therefore, an Identity Theft Risk Analysis (see Appendix A) must be conducted by the Agency Privacy Officer to determine the risk of harm associated with the breach/potential breach. Adverse affect, or risk of harm, is implicitly part of the concept of breach. As a general rule, the risk of harm to the individual is higher when the sensitivity of the data involved is greater. In addition to the risk of harm that is likely to occur, the relative likelihood of the risk occurring (risk level) will be established.

b. The findings of this assessment must be reported to the SPO, who will determine if notification is required. If notification is required, refer to paragraph 8-4.

c. If the risk assessment determines notification is not required, the rationale must be documented.

8-4. NOTIFICATION TO IMPACTED INDIVIDUAL(S).

a. Notification to the affected individual(s) shall be made as soon as possible, but not later than 10

working days after the loss, theft, or compromise is discovered and the identities of the individual(s) ascertained.

b. Notification may be delayed for good cause; however, when the notification is not made within the 10-day period, the Deputy Secretary of Defense must be informed why notice was not provided within the 10-day period. This notice must be provided to the Director, Defense Privacy Office, who must then notify the OMB Director of Administration and Management.

c. Notification to affected individual(s) shall be in writing and should be concise, conspicuous, and in plain language. The following elements shall be included:

(1) Briefly describe the facts and circumstances surrounding the loss, theft, or compromise.

(2) Describe the types of personal information involved in the breach (e.g. full name, SSN, date of birth, home address, account number).

(3) State whether the information was encrypted or protected by other means if it is determined that such information would be beneficial and would not compromise the security of the system.

(4) As a courtesy, provide contact information for government-wide services, such as USA Services, to provide support in protecting themselves from potential harm.

(5) Inform the individual(s) what the Agency is doing to investigate the breach, to mitigate losses, and to protect against further breaches.

(6) Provide Agency contact information to include phone number, e-mail address, and postal address.

d. The preferred method of notification is by first-class mail; however, other means, such as telephone, e-mail, and substitute notice, may also be employed depending on the number of individuals affected, what contact information is available, and the urgency associated with a particular breach.

e. Follow-up written notification will be given when telephonic notification is effected. The front of the envelope should be labeled to alert the recipient to the importance of its contents, e.g., “Data Breach Information Enclosed” and shall be marked as “provided in accordance with the OMB guidance.” The envelope must include the DeCA return address.

f. If the affected individual(s) cannot readily be identified or if the affected individual(s) cannot be reached, a generalized (substitute) notice should be given to the potentially impacted population by whatever means is most likely to reach the impacted individual(s).

8-5. MEDIA NOTIFICATIONS. While the first consideration must be to notify the affected individual(s), further consideration should be given to notifying possible other third parties, such as the media, when failure to do so may possibly erode public trust. The actions taken to inform the media are necessary to preserve the public’s confidence in how DeCA does business.

a. Media notifications must be promptly prepared in cases where the breach is significant (i.e., impacting thousands of individuals, the information is highly sensitive) and the risks and potential for harm to the individuals involved as a result of the breach are greater than the risks and potential for harm

to the investigation as a result of public disclosure of the breach. Early preparation ensures that the Agency can readily respond to a media inquiry or when determined necessary, release information to media organizations.

b. A protocol to determine when a public affairs release on a breach should be made on a case-by-case basis and the Director of DeCA will make the determination to release the public announcement.

8-6. ADMINISTRATIVE/DISCIPLINARY ACTION. In appropriate circumstances, the SPO should recommend to management that administrative or disciplinary action may be warranted and appropriate for those individuals determined to be responsible for the breach, loss, theft, or compromise. In evaluating the potential disciplinary action, management should consult with the SPO to determine appropriate action to correct the deficiencies/deficiency.

CHAPTER 9

PENALTIES FOR NONCOMPLIANCE

9-1. CRIMINAL AND CIVIL PENALTIES. Penalties for noncompliance with the Privacy Act may be imposed on agencies as well as individuals.

a. Criminal misdemeanor fines of up to $5,000 may be imposed on individual employees who:

(1) Knowingly and willfully disclose PII to any person not entitled to access.

(2) Maintain a system of records without meeting public notice requirements.

(3) Knowingly and willfully request or obtain records under false pretenses.

b. Civil penalties, to include payment of actual damages and/or reasonable attorney's fees, may be imposed on agencies for:

(1) Failing to comply with any Privacy Act provision or Agency rule that results in adverse effect.

(2) Failing to maintain accurate, relevant, timely, and complete data.

(3) Refusing to amend a record, as required by law.

(4) Refusing to grant legal access to records.

9-2. ADMINISTRATIVE DISCIPLINARY SANCTIONS. 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

CHAPTER 10

ACCESS BY INDIVIDUALS

10-1. INCORPORATION OF CHAPTER 3, DoD 5400.11-R BY REFERENCE. The provisions of Chapter 3, Access by Individuals, of DoD 5400.11-R (Reference (j)), are incorporated herein by reference. Nothing contained herein shall be construed to limit the applicability of the principles and procedures for access and amendment set forth in Reference (j), but are to be construed solely as supplementing those principles and procedures.

10-2. INDIVIDUAL REQUEST FOR ACCESS AND AMENDMENT. Individuals shall address requests for access to or amendment of records about themselves in a system of records to the Privacy Officer, Defense Commissary Agency, 1300 E Avenue, Fort Lee, VA 23801-1800, (804) 734-8000, ext. 48116; by fax at (804) 734-8259; or by e-mail to FOIA@DeCA.mil.

10-3. INDIVIDUAL ACCESS. Individuals may seek access to records about themselves that are maintained in a system of records in accordance with the procedures of this Chapter and of Chapter 3 of Reference (j).

a. Before granting access to personal data, an individual may be required to provide reasonable proof of his or her identity. Proof of identity is normally provided by documents that an individual ordinarily possesses, such as a common access card, military identification, driver's license. If a request for access is submitted by mail, that request should contain sufficient identifying information known only to the requester, such as full name, place and date of birth, to locate the records sought. An unsworn declaration under penalty of perjury is an acceptable means of proving the identity of an individual.

b. If an individual wishes to be accompanied by a third-party when seeking access to his or her records, or to have the records directly released to a third party, the individual may be required to furnish a signed access authorization granting the third party access.

c. An individual shall not be refused access to his or her record solely because he or she refuses to provide his or her SSN, unless the SSN is the only method by which retrieval can be made.

d. An individual is not required to explain or justify his or her need for access to any record containing personal information about him- or herself.

e. An individual will be granted access to the original record or an exact copy of the original without changes or deletions, unless not readily available due to deteriorated state or if information contained in the record is exempt from release. In such cases, an extract may be prepared for release.

f. Requesters who seek access to records about themselves that are not contained in a Privacy Act system of records, will have their requests processed under FOIA in accordance with References (k), (l) and (m).

g. Normally, access will be provided within 20 working days after receipt of the request. If access cannot be given within the 20 working day period, the requester shall be notified in an interim response.

10-4. DENIAL OF INDIVIDUAL ACCESS.

a. An individual may be denied access to a record pertaining to him or her in accordance with the provisions and procedures of paragraph C3.2 of Reference (j).

b. Access may be denied if the record was compiled in anticipation of a civil action or proceeding if the record is in a system of records that has been exempted from the access provisions under a permitted exemption if the record contains classified information that has been exempt from the access provisions under the blanket exemption for such material claimed for all DoD record systems, if another federal statute permits denial, or for other reasons as set forth in Reference (j)

c. Access may also be denied if the record is not described well enough to enable it to be located with a reasonable amount of effort or if the individual refuses to comply with established procedural requirements.

d. If access is to be denied, the DeCA SPO shall notify the requester in writing of the specific reason for the denial, of the requester's right to appeal the denial within 60 calendar days, and the title and address of the DeCA Appeal Authority.

e. An appeal of a denial of access should be processed within 30 days of receipt unless the appeal authority determines that a fair and equitable review cannot be made within that period. If additional time for review is needed, the requester should be notified in writing of the reasons for the delay and of the expected date that the requester can expect a determination. After a determination regarding an appeal has been made, the requester shall be notified in writing of the exact reason for the denial and of his or her right to seek judicial review

f. The DeCA Denial Authority is the DeCA SPO.

g. The DeCA Appeal Authority is the COS.

10-5. AMENDMENT OF RECORDS.

a. Requests for the amendment of any record pertaining to an individual contained in a system of records shall be processed in accordance with the procedures and provisions of paragraph C3.3, Amendment of Records, of Reference (j).

b. Normally, amendments are limited to correcting factual matters and not matters of official judgment, such as performance ratings, promotion potential, and job performance appraisals. Amendments are not intended to permit the alteration of records presented in the course of judicial or quasi-judicial proceedings, nor are amendments intended or designed to permit a collateral attack upon what has already been the subject of a judicial or quasi-judicial determination.

c. Requests for amendment should be in writing and should include the following:

(1) A description of the item or items to be amended.

(2) The specific reason for the amendment.

(3) The type of amendment action sought (deletion, correction, or addition).

(4) Copies of available documentary evidence supporting the request.

d. If amendment is to be denied, the DeCA SPO shall notify the requester in writing of the specific reason for the denial, of the requester's right to appeal the denial within 60 calendar days, and the title and address of the DeCA Appeal Authority.

e. An appeal of a denial of amendment should be processed within 30 days of receipt unless the appeal authority determines that a fair and equitable review cannot be made within that period. If additional time for review is needed, the requester should be notified in writing of the reasons for the delay and of the expected date that the requester can expect a determination. After a determination regarding an appeal has been made, the requester shall be notified in writing of the exact reason for the denial and of his or her right to seek judicial review

f. The DeCA Denial Authority is the DeCA SPO.

g. The DeCA Appeal Authority is the COS.

APPENDIX A

RISK ASSESSMENT MODEL

No.	Factor	Risk Determination	Low: Moderate: High:	Comments: All breaches of PII, whether actual or suspected, require notification to U.S. CERT. Low and moderate risk/harm determinations and the decision whether notification of individuals is made, rest with the head of the DoD Component where the breach occurred. All determinations of high risk or harm require notifications.
1.	**What is the nature of the data elements breached? What PII was involved?**			
	a. Name only.	Low		Consideration needs to be given to unique names; those where one or only a few in the population may have or those that could readily identify an individual; i.e., public figure.
	b. Name plus one or more personal identifier (not SSN, medical or financial).	Moderate		Additional identifiers include date and place of birth, mother's maiden name, biometric record, and any other information that can be linked or is linkable to an individual.
	c. SSN	High		
	d. Name plus SSN.	High		
	e. Name plus medical or financial data.	High		
2.	**Number of individuals affected.**			The number of individuals involved is a determining factor in how notifications are made, not whether they are made.
3.	**What is the likelihood the information is accessible and usable? What level of protection applied to this information?**			
	a. Encryption (FIPS 140-2.)	Low		
	b. Password.	Moderate/High		Moderate/High determined in relationship to category of data in No. 1.
	c. None	High		
4.	**Likelihood the breach may lead to harm.**	High/Moderate/ Low		Determining likelihood depends on the manner of the breach and the type(s) of data involved.
5.	**Ability of the Agency to mitigate the risk of harm.**			
	a. Loss	High		Evidence exists that PII has been lost; no longer under DoD control.
	b. Theft	High		Evidence shows that PII has been stolen and could possibly be used to commit ID theft?
	c. Compromise			
	(1) Compromise within DoD control.	Low High		No evidence of malicious intent. Evidence or possibility of malicious intent.

	(2) Compromise beyond DoD control.	High		Possibility that PII could be used with malicious intent or to commit identification theft.

[DoD Components are to thoroughly document the circumstances of all breaches of PII and the decisions made relative to the factors above in reaching their decision to notify or not notify individuals.]

APPENDIX B

REMOVAL OF PRIVACY DATA FROM WORKPLACE

I propose to remove the following data from the workplace:

_____

This data is maintained in/on

Files located in the office of:_____

Hard drive of PC belonging to: _____

Records maintained in the IT system: _____

The reason for removal of this information is:

_____

The expected date and/or time for return of this information to the workplace is:

_____

I acknowledge, understand, and agree that all Privacy Act materials must be stored in a secure location (e.g., locked filing cabinet, in a locked room) at all times and agree to abide by this.

_____ _____
(Signature) (Print Name)

_____ _____
(Supervisor Signature) (Print Supervisor Name)

_____ _____
(Date) (Office)

GLOSSARY

DEFINITIONS

breach. A loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII whether physical or electronic.

individual. A living person who is a citizen of the United States or an alien lawfully admitted for permanent residence. The parent of a minor or the legal guardian of any individual also may act on behalf of an individual, except as otherwise provided in Reference (g). Members of the United States Armed Forces are "individuals." Corporations, partnerships, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities are not "individuals" when acting in an entrepreneurial capacity with DoD, but persons employed by such organizations or entities are "individuals" when acting in a personal capacity (e.g., security clearances, entitlement to DoD privileges or benefits).

personal information. Information about an individual that identifies, links, relates, or is unique to; or describes him or her (e.g., SSN; age; marital status; race; home phone numbers; other demographic, biometric, personnel, medical, and financial information). Such information also is known as PII (e.g., information which can be used to distinguish or trace an individual's identity, such as his or her name; SSN; date and place of birth; mother's maiden name; and biometric records, including any other personal information which is linked or linkable to a specified individual).

personally identifiable information (PII). A combination of information about an individual person, including, but not limited to, education, financial transactions, medical history, criminal history, employment history and an individual identifier (i.e., information which can be used to distinguish or trace that individual's identity, such as their name, SSN, date and place of birth, mother's maiden name, including any other personal information which is linked or linkable to an individual). Records that contain personal information but do not include an individual identifier are not considered PII**.**

record. Any item, collection, or grouping of information, whatever the storage media (e.g., paper, electronic), about an individual that is maintained by a DoD Component, including, but not limited to, his or her 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 fingerprint, a voice print, or a photograph.

system manager (SM). The individual who is responsible for maintaining the group of records, whether paper file records or electronic records, containing personal information.

system of records. A group of records under the control of a DoD Component from which personal information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to an individual.

System of Records Notice (SORN). A notice, published in the Federal Register, that advises the public of the type of data an Agency plans to collect, how the data will be used and safeguarded, who will have access, and various other details**.**

GLOSSARY

ACRONYMS

CEO	Chief Executive Officer
COS	chief of staff
DeCAD	Defense Commissary Agency Directive
DeCAM	Defense Commissary Agency Manual
DGC	Deputy General Counsel
DoD	Department of Defense
DSN	Defense Switched Network
fax	facsimile
FOIA	Freedom of Information Act
FPO/SSG	functional process owners/special staff group
GC	General Counsel
GRS	General Records Schedule
IT	information technology
OMB	Office of Management and Budget
PIA	privacy impact assessment
PII	personally identifiable information
PO	privacy officer
POC	point of contact
SM	system manager
SORN	System of Records Notice
SPO	senior privacy official
SSN	Social Security number
TDY	temporary duty
U.S.C.	United States Code
U.S. CERT	United States Computer Emergency Readiness Team