



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

MANUAL

Privacy Act Program Manual

DeCAM 80-21.1
July 2, 2009

General Counsel
OPR: DeCA/GC

- 1. POLICY.** This Manual is issued under the authority of Defense Commissary Agency (DeCA) Directive (DeCAD) 80-21 (Reference (a)) and 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 (b)), in accordance with provisions of DOD Directive 5400.11 (Reference (c)).
- 3. APPLICABILITY.** This Manual applies to all DeCA activities.
- 4. MANAGEMENT CONTROL SYSTEM.** This Manual does not contain internal management control provisions that are subject to evaluation, testing, and other requirements of DeCAD 70-2 (Reference (d)) and as specified by the Federal Manager' 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

REFERENCES	4
Chapter 1 – Introduction	
1-1 Purpose	5
1-2 Background	5
1-3 Privacy Act Program Mission	5
1-4 Feedback.....	5
Chapter 2 – Handling/Safeguarding Privacy Act Data	
2-1 General	6
2-2 Collecting Privacy Data.....	6
2-3 Storing Privacy Data	6
2-4 Sharing/Handling Privacy Data.....	7
2-5 Removing Privacy Data.....	7
2-6 Transmitting Privacy Data.....	8
2-7 Disposal of Privacy Data.....	9
Chapter 3 – Training	
3-1 Purpose	10
3-2 Privacy Awareness	10
3-3 Training	10
Chapter 4 – System of Records Notice (SORN) Requirements	
4-1 Purpose	11
4-2 System Manager (SM) Responsibilities	11
4-3 Evaluation of Proposed System of Records	12
4-4 Preparation of System Notice.....	12
4-5 Altered Records Systems.....	13
4-6 Penalties for Noncompliance.....	13
Chapter 5 – Privacy Impact Assessments (PIA)	
5-1 Purpose	14
5-2 Office of Responsibility	14
Chapter 6 – Privacy Act Statements	
6-1 Purpose	15
6-2 How to prepare a Privacy Statement	15
Chapter 7 – Breach Procedures	
7-1 Purpose	17

7-2	Reporting Inappropriate Disclosures	17
7-3	Risk Analysis to Determine if Impacted Individual(s) Should Be Notified.....	18
7-4	Notification to Impacted Individual(s)	18
7-5	Media Notifications	19
7-6	Administrative/Disciplinary Action	20

Chapter 8 – Penalties for Noncompliance

8-1	Civil and Criminal Penalties.....	21
8-2	Administrative and Disciplinary Sanctions	21

APPENDICES

Appendix A	Risk Assessment Model	22
Appendix B	Removal of Privacy Data from Workplace	24

GLOSSARY

Definitions	25
Acronyms	26

REFERENCES

- (a) DeCA Directive 80-21, "Privacy Act Program," June 18, 2009
- (b) Section 552a of Title 5, United States Code, "The Privacy Act of 1974," as amended
- (c) DOD Directive 5400.11, "DOD Privacy Program," May 8, 2007
- (d) DeCA Directive 70-2, "Internal Control Program," December 17, 2007
- (e) Office of Management and Budget Circular No. A-130, Appendix I, "Federal Agency Responsibilities for Maintaining records About Individuals"
- (f) Public Law 107-347, 116 Stat. 2899, "E-Government Act of 2002," December 17, 2002
- (g) Executive Order 9397, "Numbering System for Federal Accounts Relating to Individual Persons," November 22, 1943
- (h) OSD Policy Memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," September 21, 2007
- (i) DOD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
- (j) DOD 5200.1-R, "Information Security Program", January 1997
- (k) DOD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
- (l) DeCA Directive 30-18, "Defense Commissary Agency Security Programs," March 1, 1997
- (m) 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 (b)). The guidance contained herein applies to all DeCA activities and all DeCA personnel. All references to Privacy contained throughout this Manual pertain to Reference (b). 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 (c) and is to be used in coordination with Department of Defense (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 (b). 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

HANDLING/SAFEGUARDING PRIVACY ACT DATA

2-1. 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.

2-2. 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.

2-3. 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 2-6 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 4.
 - (2) Privacy Act Statement guidelines defined in Chapter 6.

2-4. 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 System of Records Notice (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.

2-5. 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/Freedom of Information Act (FOIA), or Senior Privacy Official (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.

2-6. 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 "Sensitive Unclassified Information" cover sheet (DeCAF 30-34) or "Privacy Act Data Cover Sheet" (DD Form 2923).

(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.

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.

2-7. 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 3

TRAINING

3-1. 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 (b). 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 non-compliance.

3-2. 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.

3-3. 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 4

SYSTEM OF RECORDS NOTICE (SORN) REQUIREMENTS

4-1. 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.

4-2. 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 (a).

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 (e)).

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

4-3. 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.

4-4. 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 all 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 4-5) or revising any existing record system, the system must first be reviewed and evaluated (Paragraph 4-3) to determine if the SORN must also be revised.

4-5. 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 (b).

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

4-6. 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 8 for details.

CHAPTER 5

PRIVACY IMPACT ASSESSMENTS (PIA)

5-1. PURPOSE. Section 8 of the E-Government Act of 2002 (Reference (f)) establishes requirements for conducting, reviewing, and publishing PIAs 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.

5-2. OFFICE OF RESPONSIBILITY. The office of primary responsibility for PIAs is the Chief Information Officer.

CHAPTER 6

PRIVACY ACT STATEMENTS

6-1. 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.

6-2. 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 (g)) 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 7

BREACH PROCEDURES

7-1. 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 (f)).

7-2. 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/functional process owner/special staff group Privacy point of contact as soon as possible after other required notifications have been accomplished.

7-3. RISK ANALYSIS TO DETERMINE IF IMPACTED INDIVIDUAL(S) SHOULD BE NOTIFIED. 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.

- a. 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 7-4.
- b. If the risk assessment determines notification is not required, the rationale must be documented.

7-4. 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, etc., 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).

7-5. 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.

7-6. 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 8

PENALTIES FOR NONCOMPLIANCE

8-1. 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.

8-2. 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.

APPENDIX A

RISK ASSESSMENT MODEL

No.	Factor	Risk Determination	<p>Low: Moderate: High:</p>	<p>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.</p>
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 (f). 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, etc., 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

DeCAD	Defense Commissary Agency Directive
DSN	Defense Switched Network
fax	facsimile
FOIA	Freedom of Information Act
GC	General Counsel
GRS	General Records Schedule
IT	information technology
OMB	Office of Management and Budget
PIA	privacy impact assessment
PII	personally identifiable information
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