

**Army Regulation 25–22**

**Information Management**

# **The Army Privacy Program**

**Headquarters  
Department of the Army  
Washington, DC  
22 December 2016**

**UNCLASSIFIED**

# ***SUMMARY of CHANGE***

AR 25–22

The Army Privacy Program

This major revision, dated 22 December 2016—

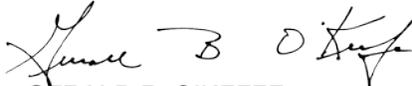
- o Adds discussion of general provisions and special handling provisions (chap 1).
- o Updates the responsibilities of senior officials as necessary (chap 2).
- o Updates the information on systems of records, privacy impact assessments, and blanket routine uses (chap 3).
- o Revises information on exemptions; provides a link to the Records Management and Declassification Agency Web site for most of the detailed information including the current listing of system of records notices (chap 4).
- o Updates the information on handling and safeguarding personally identifiable information (chap 5).
- o Clarifies the relationship between the Privacy Act and the Freedom of Information Act (para 6–5).
- o Revises information on disclosure of personal information to other agencies and third parties (chap 7).
- o Adds information on Privacy Act Review Board appeals (chap 8).
- o Adds information on breach reporting, risk assessment, notifications, and mitigation (chap 9).
- o Adds information on Privacy Act complaints (chap 10).
- o Adds information on Privacy Act training requirements and resources (chap 11).
- o Restructures content; removes outdated procedural, historical, and background information; and updates paragraphs with authoritative documents and Web sites (throughout).

Information Management  
The Army Privacy Program

By Order of the Secretary of the Army:

MARK A. MILLEY  
General, United States Army  
Chief of Staff

Official:



GERALD B. O'KEEFE  
Administrative Assistant to the  
Secretary of the Army

**Proponent and exception authority.**

The proponent of this regulation is the Administrative Assistant to the Secretary of the Army. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

**Army internal control process.** This regulation contains internal control provisions in accordance with AR 11–2 and

identifies key internal controls that must be evaluated (see appendix F).

**Supplementation.** Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Office of Administrative Assistant to the Secretary of the Army, (AAHS-RDF), Fort Belvoir, VA 22060-5605.

**Suggested improvements.** Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Administrative Assistant to the Secretary of the Army (AAHS-RDF), Fort Belvoir, VA 22060-5605.

**Distribution.** This publication is available in electronic media only and is intended for command levels B, C, D, and E for the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

**History.** This publication is a major revision.

**Summary.** This regulation on the Army Privacy Program has been revised. It supplements DOD Directive 5400.11.

**Applicability.** This regulation applies to the Active Army, the Army National Guard/Army National Guard of the United States, the U.S. Army Reserve, and the Army and Air Force Exchange Service.

**Contents** (Listed by paragraph and page number)

**Chapter 1**

**General Information, page 1**

Purpose • 1–1, page 1

References • 1–2, page 1

Explanation of abbreviations and terms • 1–3, page 1

Responsibilities • 1–4, page 1

Legal authority • 1–5, page 1

Overview • 1–6, page 1

Fair Information Practice Principles • 1–7, page 1

General provisions • 1–8, page 2

Special handling provisions • 1–9, page 3

**Chapter 2**

**Responsibilities, page 4**

The Administrative Assistant to the Secretary of the Army • 2–1, page 4

The Judge Advocate General • 2–2, page 5

The General Counsel • 2–3, page 5

\*This regulation supersedes AR 340–21, dated 5 July 1985.

## Contents—Continued

Heads of Headquarters, Department of Army staff and Army commands • 2–4, *page 5*

### Chapter 3

#### **Systems of Records, Privacy Impact Assessments, and Department of Defense Routine Uses, *page 7***

Privacy Act systems of records • 3–1, *page 7*

Privacy impact assessment • 3–2, *page 8*

Department of Defense blanket routine uses • 3–3, *page 8*

Computer matching • 3–4, *page 10*

### Chapter 4

#### **Exemptions, *page 10***

Exempting systems of records • 4–1, *page 10*

General exemption • 4–2, *page 10*

Specific exemptions • 4–3, *page 10*

Army systems of records notices citing exemptions • 4–4, *page 11*

### Chapter 5

#### **Handling and Safeguarding Personally Identifiable Information, *page 11***

Collecting personally identifiable information • 5–1, *page 11*

Safeguarding personally identifiable information • 5–2, *page 12*

Protecting social security numbers • 5–3, *page 13*

### Chapter 6

#### **Individual Access to Records and Denials, *page 13***

Individual access applicability • 6–1, *page 13*

Individual requests for access • 6–2, *page 13*

Individual access to medical records • 6–3, *page 14*

Personal notes • 6–4, *page 14*

Relationship between Privacy Act and Freedom of Information Act • 6–5, *page 14*

Denial authorities • 6–6, *page 15*

Fees • 6–7, *page 16*

### Chapter 7

#### **Disclosure of personal records to other agencies and third parties, *page 16***

Disclosure to third parties • 7–1, *page 16*

Disclosure accounting • 7–2, *page 17*

### Chapter 8

#### **Amending Records and Department of the Army Privacy Act Review Board, *page 18***

Periodic review and amendment of records • 8–1, *page 18*

Department of the Army Privacy Act Review Board appeal process • 8–2, *page 19*

Department of the Army Privacy Act Review Board meetings • 8–3, *page 19*

### Chapter 9

#### **Breach Reporting, Risk Assessment, Notification, and Mitigation, *page 20***

Breach process • 9–1, *page 20*

Risk assessment and notification determination • 9–2, *page 20*

Notification timelines • 9–3, *page 22*

Means of providing notification • 9–4, *page 22*

Risk mitigation • 9–5, *page 23*

Completion of Privacy Act Tracking System submission • 9–6, *page 23*

Additional breach reporting resources • 9–7, *page 24*

### Chapter 10

#### **Privacy Act Complaints and Judicial Sanctions, *page 24***

Privacy Act complaints • 10–1, *page 24*

Judicial sanctions • 10–2, *page 24*

## Contents—Continued

### Chapter 11

#### **Training Requirements and Resources**, *page 25*

Training requirements • 11-1, *page 25*

Training records • 11-2, *page 25*

Training materials • 11-3, *page 25*

Conceptual training • 11-4, *page 25*

### Appendixes

A. References, *page 27*

B. Denial Authorities, *page 32*

C. Exempt Army and Office of Personnel Management Records, *page 34*

D. Privacy Act Statement, *page 55*

E. System of Records Notice Samples, *page 56*

F. Internal Control Evaluation, *page 64*

### Figure List

Figure D-1: Privacy Act Statement Structure, *page 55*

Figure E-1: Example of a System of Records Notice, *page 59*

Figure E-1: Example of a System of Records Notice—continued, *page 59*

Figure E-1: Example of a System of Records Notice—continued, *page 59*

Figure E-2: Army System of Records Notice Checklist, *page 60*

Figure E-3: Army System of Records Notice Narrative Statement, *page 63*

Figure E-3: Army System of Records Notice Narrative Statement—continued, *page 63*

### Glossary



## **Chapter 1**

### **General Information**

#### **1–1. Purpose**

The purpose of the Army Privacy Program is to balance the Government’s need to maintain information about individuals with the right of individuals to be protected against unwarranted invasions of their privacy stemming from the collection, maintenance, use, or disclosure of personal information. This regulation sets forth policies and procedures that govern personal information kept by the Department of the Army (DA) in Privacy Act systems of records. This regulation also provides general guidance on collecting, safeguarding, and disclosing personal information. Additionally, this regulation promotes uniformity within the Army’s Privacy Program.

#### **1–2. References**

See appendix A.

#### **1–3. Explanation of abbreviations and terms**

See the glossary.

#### **1–4. Responsibilities**

See chapter 2 for responsibilities.

#### **1–5. Legal authority**

The Privacy Act of 1974, as amended, Title 5, United States Code, section 552a (5 USC 552a) is the statutory basis for the Army Privacy Program. Within the Department of Defense (DOD), the Act is implemented by DODD 5400.11 and DOD 5400.11–R. The Act assigns—

- a.* Overall Government-wide responsibilities for implementation to the Office of Management and Budget (OMB).
- b.* Specific responsibilities to the Office of Personnel Management (OPM) and the General Services Administration (GSA).

#### **1–6. Overview**

The Army maintains records during the conduct of Army business. Army records, regardless of media, are maintained from creation through final disposition in a manner that protects the rights and interests of individuals and the Federal Government. In general, the Army observes the fair information practice principles of awareness, consent, access, security, and enforcement. Individuals are aware of what personal information is maintained about them; they must explicitly give their consent when they provide personal information; they have access to personal information based on fair practices and procedures; their personal information is stored in a secure manner; and any breach of personal information security will be handled with necessary enforcement. Army administrative and operational activities involve the handling and safeguarding of personally identifiable information (PII). Life-cycle management of Army records is governed by AR 25–400–2.

*a.* The Privacy Official for each Army activity provides a Privacy Act Statement (PAS) to individuals whenever collecting information that will be maintained in a Privacy Act system of records (SOR), regardless of the medium used to collect the information (for example, forms, personal interviews, telephonic interviews, and other methods).

*b.* An Army organization will not maintain a record describing how an individual exercises First Amendment rights unless collection and maintenance of this information is within the scope of an authorized law enforcement activity, expressly covered by Federal statute, or explicitly provided by the subject individual. First Amendment rights include religious and political beliefs, freedom of speech and the press, and the rights of assembly and petition.

#### **1–7. Fair Information Practice Principles**

The FIPP, originally developed in 1973 by the Department of Health, Education, and Welfare, formed the conceptual core for the Privacy Act of 1974. These principles are used by the Army when handling records containing PII:

*a. Transparency.* The Army will promote transparency and accountability by providing notice to the individual regarding its maintenance of PII.

*b. Individual participation.* The Army will involve individuals in the process of using their PII and, to the extent practicable, seek individual consent for the maintenance of their PII. The Army will also provide mechanisms for appropriate access, amendment, and redress regarding the Army’s use of their PII.

*c. Purpose specification.* The Army will state the authorities that permit the collection of PII, as well as the purpose or purposes for which the PII is to be used. The purpose specification will be directly related to the purpose stated in the authorities.

*d. Data minimization.* The Army will only collect PII that is directly relevant and necessary to accomplish a specified purpose, and only retain PII for as long as is necessary to fulfill the specified purpose.

*e. Use limitation.* The Army will limit the use of PII solely to the purpose specified in the applicable system of records notice. Sharing PII outside the Army must be for a purpose compatible with the purpose for which the PII was collected.

*f. Data quality and integrity.* The Army will, to the greatest extent practicable, ensure that PII is timely, accurate, complete, and relevant.

*g. Security.* The Army will protect PII in all media through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

*h. Accountability and auditing.* Army personnel and contractors must be accountable for complying with these principles and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

## **1–8. General provisions**

General provisions of the Privacy Act include protecting individual privacy rights, safeguarding of personal information, conveying privacy data electronically via email and the World Wide Web, protecting records containing personal identifiers such as name and social security number (SSN), and notifying individuals when personal information is lost, stolen, or compromised, and Federal Government contractor compliance. This section describes each category of provisions.

*a. Individual privacy rights policy.* Army policy concerning the privacy rights of individuals and the Army's responsibilities for compliance with the Privacy Act are as follows:

(1) Protect the privacy of living U.S. citizens and aliens lawfully admitted for permanent residence from unwarranted intrusion.

(2) Although deceased individuals do not have Privacy Act rights, Family members or next-of-kin may have limited privacy rights with respect to the release of information regarding the death and the funeral arrangements of the deceased individual. Family members often use the deceased individual's SSN or DOD identification data (ID) number for Federal entitlements. Also, the Health Insurance Portability and Accountability Act (HIPAA) extends protection to certain medical information contained in a deceased individual's medical records. Appropriate safeguards must be implemented to protect the deceased individual's PII and protected health information (PHI).

(3) PHI of individuals, both living and deceased, will not be used or disclosed except as authorized by law or regulation. Management of medical records is governed by AR 40–66.

(4) Maintain only such information about an individual that is necessary to accomplish the Army's mission.

(5) Ensure that personal information is timely, accurate, complete, and relevant to the collection purpose.

(6) Safeguard personal information to prevent unauthorized use, access, disclosure, alteration, or destruction.

(7) Maintain records for the minimum time required in accordance with AR 25–400–2 which mandates use of the Army records retention schedule according to National Archives and Records Administration (NARA) record disposition instructions.

(8) Let individuals know what Privacy Act records the Army maintains by publishing systems of records notices in the Federal Register (FR). A SOR is a group of records under the control of DA from which PII about an individual is retrieved by the individual's name or identifying number, symbol, or other unique identifier. DA systems of records notices are available at the Records Management and Declassification Agency (RMDA) Web site: <https://www.rmda.army.mil/privacy/sorns/>.

(9) Permit individuals to correct and amend records about themselves which they can prove are untimely, inaccurate, incomplete, or irrelevant.

(10) Allow individuals to request an administrative review of decisions that deny them access to or the right to amend their records.

(11) Act on all requests promptly, accurately, and fairly.

(12) Keep paper and electronic records that are retrieved by name or personal identifier only in approved Privacy Act systems of records.

(13) Do not maintain records describing how an individual exercises his or her rights guaranteed by the First Amendment (freedom of religion, freedom of political beliefs, freedom of speech and press, freedom of peaceful assembly, and petition) unless expressly authorized by statute, pertinent to and within the scope of an authorized law enforcement activity, or otherwise authorized by law or regulation.

(14) Maintain appropriate administrative technical and physical safeguards to ensure records are protected from unauthorized alteration or disclosure.

(15) Otherwise comply with EO 12333 and DOD directives.

*b. Personal information guidelines.* Safeguard personal information according to the following guidelines:

(1) Privacy Act data will be afforded reasonable safeguards to prevent inadvertent or unauthorized disclosure of records during processing, storage, transmission, and disposal.

(2) Shared drives containing personal information should be protected so only those with official “need to know” have access to the information during the performance of official duties.

(3) Safeguarding methods must strike a balance between the sensitivity of the data, need for accuracy and reliability for operations, general security of the area, and cost of the safeguards. In some situations, a password may be enough protection for an automated system with a log-on protocol. For additional guidance on safeguarding personal information in automated records, see AR 25–2.

### **1–9. Special handling provisions**

*a.* Convey privacy protected data electronically via email and the World Wide Web according to the following guidelines:

(1) All PII transmitted electronically should be encrypted. Unencrypted electronic transmission of privacy protected data makes the Army vulnerable to information interception which can cause serious harm to the individual and jeopardize the accomplishment of the Army’s mission.

(2) The Privacy Act requires that appropriate technical safeguards be established, based on the media used to ensure the security of the records and to prevent compromise or misuse during transfer (for example, paper, electronic).

(3) Privacy Web sites and hosted systems with privacy-protected data will employ secure sockets layer and Public Key Infrastructure (PKI) encryption certificates or other DOD-approved commercially available certificates for server authentication and client and/or server authentication. Individuals who transmit data containing PII over email must use PKI or other DOD-approved certificates.

(4) Add appropriate privacy and security notices at major Web site entry points. Refer to AR 25–1 for requirements on posting privacy and security notices on public Web sites. Procedures related to the establishing, operating, and maintaining of unclassified DA Web sites can be accessed at: <http://www.defense.gov/webmasters/>.

(5) Ensure public Web sites comply with policies regarding restrictions on persistent and third-party cookies. The Army prohibits both persistent and third-party cookies.

(6) Add a Privacy Act Advisory (PAA) on Web sites with host information systems soliciting personally identifiable information, even when not maintained in a Privacy Act SOR. The PAA informs the individual as to why the information is being solicited and how it will be used. Post the PAA on the Web site where the information is being solicited, or to a well-marked hyperlink. Example wording is as follows: “Privacy Act Advisory—Please refer to the Privacy and Security Notice that describes why this information is collected and how it will be used.”

(7) When sending Privacy Act protected information within the Army across encrypted or dedicated lines, ensure that—

*(a)* Each addressee has an official “need to know.” Remove any recipient without “need to know” from all addressee fields.

*(b)* Information protected by the Privacy Act is marked For Official Use Only (FOUO) to inform the recipient of limitations on further dissemination. For example, add FOUO to the beginning of an email message, along with appropriate language such as the following: “This document contains For Official Use Only (FOUO) information which is protected under the Privacy Act of 1974 and AR 25–22, The Army Privacy Program. Do not further disseminate this information without the permission of the sender.”

*(c)* Use FOUO/Privacy Act marking only in situations where protected Privacy Act information is being transmitted.

*(d)* For additional information about marking documents as FOUO, refer to AR 25–55.

*b.* Protect records containing personal identifiers such as name and SSN as follows:

(1) Only those records covered by a system of records notice may be arranged to permit retrieval by a personal identifier (for example, an individual’s name or SSN). AR 25–400–2 requires all records thus covered to include the system of record identification number on the record label to serve as a reminder that the information contained within must be safeguarded.

(2) Use DD Form 2923 (Privacy Act Data Cover Sheet) for individual records not contained in properly labeled file folders or cabinets (for example, log books or training materials).

(3) For customized cover sheets, if needed, include a statement similar to the following: “The information contained within is For Official Use Only (FOUO) and protected by the Privacy Act of 1974, as amended.”

(4) For email with an attachment, include a statement similar to the following: “If you are not the intended recipient, please delete this email including any attachments, and notify the sender that you have done so.”

c. Notify individuals when personal information is lost, stolen, or compromised as follows:

(1) Whenever an Army organization becomes aware that protected personal information has been lost, stolen, or compromised, the organization will inform the affected individuals as soon as possible, but not later than 10 days after the loss or compromise of protected personal information is discovered. This may pertain to the following categories of individuals about whom an Army organization maintains information:

(a) Service member.

(b) Civilian employee (appropriated or nonappropriated fund).

(c) Military retiree.

(d) Family member.

(e) Another individual affiliated with an Army organization (for example, a volunteer).

(f) Any member of the public.

(2) Notification may be delayed for good cause (for example, for law enforcement purposes) as described in paragraph 9–3.

(3) At a minimum, the organization will advise individuals of what specific data was involved; the circumstances surrounding the loss, theft, or compromise; and what protective actions the individual can take.

(4) If Army organizations are unable to comply with policy, they will immediately notify their superiors, who will submit a memorandum through the chain of command to the Administrative Assistant to the Secretary of the Army (AASA) to explain why the affected individuals’ personal information has been lost, stolen, or compromised.

(5) This policy is also applicable to Army contractors who collect, maintain, use, or disseminate protected personal information on behalf of the organization.

(6) For a more complete discussion of breaches and notifications, see chapter 9.

d. Monitor Federal Government contractor compliance according to the following requirements:

(1) Contractors are considered employees of the Army for the purpose of the sanction provisions of the Privacy Act during the performance of contract requirements. Disclosing records to a contractor for use in performing the requirements of an authorized DA contract is considered a valid disclosure based on an official “need to know.”

(2) Consistent with the Federal Acquisition Regulations (FAR), contracts requiring the maintenance of a system of records or a portion of a system of records will include in the solicitation and resulting contract, such terms as prescribed by subpart 24.1 of the FAR Protection of Individual Privacy clause.

## **Chapter 2 Responsibilities**

### **2–1. The Administrative Assistant to the Secretary of the Army**

The AASA will—

a. Serve as the principal advisor to the Chief of Staff of the Army and the Secretary of the Army for the Army’s Privacy Program.

b. Coordinate with OMB, DOD, OPM, and GSA. The OMB has overall Government-wide responsibility for implementation of the Privacy Act. DOD is responsible for implementation of the Act within the Armed Services. The Privacy Act also assigns specific Government-wide responsibilities to the OPM and the GSA.

c. Implement the Army’s Privacy Program. This responsibility includes—

(1) Developing and issuing policy guidance for the program in consultation and coordination with the Army General Counsel.

(2) Ensuring that the Army’s Privacy Program complies with 5 USC 552a, as amended, DODD 5400.11, and other Federal regulations.

d. Appoint a Senior Agency Official for Privacy (SAOP) who will—

(1) Act as the SAOP with overall responsibility for the execution of the DA Privacy Program.

(2) Develop and issue policy guidance relating to information privacy.

(a) Safeguarding personally identifiable information from unauthorized use, access, and disclosure.

(b) Ensuring that all Army employees receive appropriate training and education on handling PII.

e. On behalf of the AASA, The Chief Attorney of the Office of the Administrative Assistant to the Secretary of the Army (OAASA), will—

(1) Provide advice and assistance on legal matters pertaining to the administration of the Army’s Privacy Program.

(2) Serve as the legal advisor to the DA Privacy Act Review Board. This duty may be fulfilled by a designee from the OAASA’s Office of the Chief Attorney and Legal Services.

- (3) Provide legal advice relating to interpretation and application of the Privacy Act of 1974, as amended.
- f.* Serve as a member on the Defense Privacy Board Legal Committee. This duty may be fulfilled by a designee from the OAASA's Office of the Chief Attorney and Legal Services.
- g.* On behalf of the AASA, The Chief, DA Freedom of Information Act (FOIA)/PA, U.S. Army Records Management and Declassification Agency, will—
  - (1) Develop and recommend policy.
  - (2) Execute duties for the Army's SAOP.
  - (3) Promote Privacy Act awareness throughout the DA.
  - (4) Serve as a voting member on the Defense Data Integrity Board and the Defense Privacy Board.
  - (5) Represent the Department of the Army in DOD policy meetings.
  - (6) Perform the following duties as Privacy Act Manager and head of the Army Privacy Office:
    - (a)* Administer procedures outlined in this regulation.
    - (b)* Review and approve proposed new, altered, or amended Privacy Act systems of records notices and submit them to the DPCLD for coordination.
    - (c)* Review DA forms for compliance with the Privacy Act and this regulation.
    - (d)* Ensure that reports required by the Privacy Act are provided upon request from the Army Privacy Office (the operating branch of the FOIA/PA organization).
    - (e)* Provide Privacy Act training and training resources.
    - (f)* Provide privacy guidance and assistance to Headquarters, Department of the Army and Army activities where the Army is the Executive Agent.
    - (g)* Ensure information collections are developed in compliance with Privacy Act provisions.
    - (h)* Ensure OMB reporting requirements, guidance, and policy are accomplished.
    - (i)* Immediately review privacy violations of personnel to locate the problem and develop a means to prevent recurrence of the problem.

## **2-2. The Judge Advocate General**

TJAG will—

- a.* Provide legal advice to privacy officials, commanders, and supervisors on requests for Privacy Act records under the Privacy Act and Freedom of Information Act.
- b.* Serve (via Litigation Division) as a liaison between the Army and the Department of Justice.

## **2-3. The General Counsel**

The GC will—

- a.* Develop and issue policy guidance for the Army Privacy Program, in conjunction with the AASA.
- b.* Provide a determination in writing if the DA Privacy Act Review Board determines that an amendment of the subject record is warranted.

## **2-4. Heads of Headquarters, Department of Army staff and Army commands**

HQDA staff agencies, ACOMs, ASCCs, and DRUs, as listed in AR 10-87, will—

- a.* Supervise and execute the privacy program in functional areas and activities under their responsibility.
- b.* Appoint a Privacy Official for each ACOM, in writing, and inform the Army Privacy Office of the appointment.
- c.* On behalf of the ACOMs, ASCCs, and DRUs, The Privacy Official at each activity or installation will—
  - (1) Serve as the staff advisor on privacy matters.
  - (2) Ensure that Privacy Act records collecting and maintaining PII within the ACOM are properly described in a Privacy Act system of records notice published in the FR.
  - (3) Ensure no undeclared systems of records are being maintained.
  - (4) Process Privacy Act requests promptly and responsively.
  - (5) Provide a PAS to individuals when information is collected as specified in paragraph 1-6 and appendix D.
  - (6) Review recordkeeping practices annually to ensure compliance with the Privacy Act, paying particular attention to the maintenance of automated records. In addition, ensure coordination with records management officials on such matters as maintenance and disposal procedures, statutory requirements, forms, and reports.
  - (7) Maintain narrative and statistical data for preparation of required reports (for example, Public Law 110-53 reporting for the Defense Privacy and Civil Liberties Division (DPCLD)).
  - (8) Build an adequate team of privacy officers and administrators to help with the daily workload of breach reporting, PII handling, tracking of lessons learned, training, and other privacy matters.
  - (9) Process reports of suspected Privacy Act violations.

(10) Review Privacy Act training practices annually to ensure that all personnel are familiar with the requirements of the Act. Develop and provide a privacy training program for all personnel involved in the design, development, custody, maintenance, and use of a system of records.

*d.* On behalf of the ACOMs, ASCCs, and DRUs, system and program managers will—

(1) Verify that appropriate procedures and safeguards are developed, implemented, and maintained to protect PII.

(2) Validate that all personnel are aware of their responsibilities for protecting any personal information collected or maintained under the Army Privacy Program.

(3) Ensure that each official filing system that retrieves records by name or other personal identifier and maintains those records in a Privacy Act system of records has a notice published in the FR as noted above. Any official who willfully maintains a system of records without meeting the publication requirements, as prescribed by the Privacy Act of 1974, as amended, by OMB Circular A-130, 32 CFR 310, and by this regulation, may be subject to administrative sanctions, criminal penalties, or civil lawsuits.

(4) Prepare new, amended, or altered Privacy Act systems of records notices and submit them to the Army Privacy Office for review. The Army Privacy Office assigns a system identifier and submits the document to DPCLD for review.

(5) Review each Army system of records notice biennially to ensure that it accurately describes the system of records.

(6) Review the routine use disclosures associated with each Privacy Act system of records notice based on OMB guidance in order to determine if such routine use continues to be compatible with the original collection purpose.

(7) Review each system of records notice for which the Secretary of the Army has promulgated exemption rules based on section (j) and section (k) of the Privacy Act of 1974, as amended, and OMB guidance. This review ensures such exemptions are still appropriate.

(8) Review, biennially, contracts that provide for the maintenance of a Privacy Act system of records to accomplish an activity's mission. This requirement ensures each contract contains provisions that bind the contractor, and its employees, to the requirements of 5 USC 552a(m)(1).

(9) Review, if applicable, ongoing Computer Matching Agreements. The Defense Data Integrity Board approves Computer Matching Agreements for 18 months, with an option to renew for an additional year. The renewal review ensures that the requirements of the Privacy Act, OMB guidance, and the requirements contained in the matching agreements have been met.

*e.* DA Privacy Act System and Program Managers will also ensure that DA personnel are aware of any new requirements or changes to the Army Privacy Program.

*f.* Heads of Joint Service agencies or commands for which the Army is the Executive Agent or for which the Army otherwise provides fiscal, logistical, or administrative support, will adhere to the policies and procedures in this regulation.

*g.* Chief Executive Officer, Army and Air Force Exchange Service, will supervise and execute the Privacy Program within the command according to this regulation.

*h.* DA personnel and contractors on behalf of the ACOMs, ASCCs, and DRUs will—

(1) Assist the DA in safeguarding the privacy of DA personnel and members of the public. These responsibilities, for which DA personnel and contractors are held accountable by law, prohibit:

(a) The disclosure of any record contained in a system of records by any means of communication to any person or another agency except pursuant to a written request by, or with prior written consent of, the individual to whom the record pertains or specific conditions of disclosure stated in the Privacy Act.

(b) Maintaining records describing how any individual exercises rights guaranteed by the First Amendment to the Constitution of the United States, unless expressly authorized by statute, executive order, regulation, or policy, or by the individual; or if maintenance of the information is pertinent to and within the scope of an authorized law enforcement activity.

(2) Account for all disclosure of records containing PII on individuals. Exceptions to the accounting for disclosures are:

(a) The disclosure of records containing PII to DA personnel and contractors who maintain the record and have a need for the record in the performance of their duties.

(b) The disclosure of information made in accordance with FOIA.

(3) Disclose records containing PII within the DA only to DA personnel and contractors who have a need for the record in the performance of their duties.

(4) Comply with appropriate administrative, physical, and technical safeguards to protect the privacy and confidentiality of all PII.

(5) Report to the Army Privacy Office any systems that maintain PII and are not published in an Army system of records or Government-wide system of records.

- (6) Dispose of records containing PII as soon as the information is no longer required, necessary, or useful, as permitted by the retention and disposition schedule established by NARA.
- (7) Minimize the collection of PII whenever possible.
  - i. DA personnel and contractors responsible for maintaining a system of records will—
    - (1) Ensure the maintenance of policies and practices governing the records within a system of records.
    - (2) Ensure systems of records they manage comply with the Privacy Act and all other applicable DA requirements.

## **Chapter 3**

### **Systems of Records, Privacy Impact Assessments, and Department of Defense Routine Uses**

#### **3–1. Privacy Act systems of records**

A SOR is a group of records, whatever the storage media (paper, electronic, and so forth), under the control of an Army activity from which personal information about an individual is retrieved by the name of the individual, or by an identifying number, symbol, or other identifying particular assigned, that is unique to the individual. Notices of all Army systems of records are required by the Privacy Act to be published in the FR.

- a. A notice contains—
  - (1) System name and system location for the records.
  - (2) Categories of individuals on whom records are maintained.
  - (3) Categories of records in the system.
  - (4) Authority (statutory or executive order) authorizing the system.
  - (5) Purpose of the system.
  - (6) Routine uses of the records, including categories of users and purposes of such uses.
  - (7) Policies and practices for storing, retrieving, accessing, retaining, and disposing of the records.
  - (8) Position title and business address of the responsible official.
  - (9) Procedures an individual must follow to learn if a system of records contains a record about the individual.
  - (10) Categories of sources of records in the system.
  - (11) Exemptions from the Privacy Act claimed for the system (see chap 4).
- b. New or altered systems that meet the requirements below require report to the Congress and OMB. A new system is one for which no system notice is published in the FR. An altered system is one that—
  - (1) Increases or changes the number or types of individuals on whom records are kept so that it significantly alters the character and purpose of the system of records.
  - (2) Expands the types or categories of information maintained.
  - (3) Alters the manner in which records are organized, indexed, or retrieved to change the nature or scope of those records.
  - (4) Alters the purposes for which the information is used, or adds a routine use that is not compatible with the purpose for which the system is maintained.
  - (5) Changes the equipment configuration on which the system is operated, to create potential for either greater or easier access.
- c. Report of a new or altered system should include a narrative statement. The narrative statement must contain the following:
  - (1) System identification and name.
  - (2) Responsible official title and phone number.
  - (3) Purpose of the system or nature of changes proposed (if an altered system).
  - (4) Authority for maintenance of the system.
  - (5) Probable or potential effects of the system on the privacy of individuals.
  - (6) Whether the system is being maintained, in whole or in part, by a contractor.
  - (7) Steps taken to minimize risk of unauthorized access.
  - (8) Routine use compatibility.
  - (9) Office of Management and Budget information collection requirement.
- d. System managers must send a proposed notice through their Privacy Official at least 120 days before implementing a new, amended, or altered system to the Chief, DA Freedom of Information Act and Privacy Act (FOIA/PA), 7701 Telegraph Road, Casey Building, Room 144, Alexandria, VA 22315-3827. For a sample of a completed system of records notice, a completion checklist, and a sample narrative statement, see appendix E. For additional information, see <https://www.rmda.army.mil/>.

e. Supporting documentation consists of a system notice for the proposed new or altered system and a proposed exemption rule, if applicable.

f. The existence of a statute or executive order mandating the maintenance of a system of records to perform an authorized activity does not remove the responsibility to ensure the information in the system of records is relevant and necessary to perform the authorized activity. An example is in appendix E.

g. An OMB Control Number may be required before implementation of a system of records collecting information from the public. OMB, based on the Paperwork Reduction Act of 1995, assigns control numbers for information collection requirements that are not mandated by statute. For additional information about OMB Control Numbers, see DODM 8910.01–V1.

### **3–2. Privacy impact assessment**

Privacy impact assessments (PIAs) have the following characteristics:

a. One safeguard plan is the development and use of DD Form 2930 (Privacy Impact Assessments) mandated by the E-Gov Act of 2002, section 208. The OMB directs that a PIA be prepared and published for all new or significantly altered information systems and electronic collections that collect, maintain, use, or disseminate personally identifying information. The PIA describes the appropriate administrative, technical, and physical safeguards for automated systems. The PIA assists in the protection against anticipated threats or hazards to the security or integrity of data, which could result in substantial harm, embarrassment, inconvenience, or unfairness to any subject member. Contact your local information management officer (IMO) department and refer to DODI 5400.16 for guidance on conducting a PIA.

b. The development of appropriate safeguards must be tailored to the requirements of the collection system as well as other factors such as the system environment and data accessibility.

c. Initial planning for a new or revised system of records involves an assessment of the risk of harm to economic or property interests, risk of identity theft or fraud, or potential harm to the security or integrity of the system of records. This planning analysis involves the examination of disclosure procedures and exemptions to disclosure. Any disclosure of identifiable information must be made in a manner that prevents or minimizes risk.

d. For step-by-step guidance on the completion of a PIA, see DD Form 2930 at the following Web site: <http://ciog6.army.mil/privacyimpactassessments/tabid/71/default.aspx>.

### **3–3. Department of Defense blanket routine uses**

In addition to routine uses in each system notice, the following blanket routine uses apply to all records from systems of records maintained by the Army. Disclosure exemptions apply as stated explicitly or as applicable in a general way (for example, certain law enforcement, judicial, or Congressional exceptions).

a. *Law enforcement routine use.* If an Army system of records maintained to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or related order, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether Federal, State, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the associated statute, rule, regulation, or order issued.

b. *Disclosure when requesting information routine use.* A record from an Army system of records may be disclosed as a routine use to a Federal, State, or local agency maintaining civil, criminal, or other relevant enforcement information, or other pertinent information, such as current licenses, if necessary to obtain information relevant to an Army decision concerning—

- (1) Hiring or retention of an employee.
- (2) Issuance of a security clearance.
- (3) Letting of a contract.
- (4) Issuance of a license, grant, or other benefit.

c. *Disclosure of requested information routine use.* A record from an Army system of records may be disclosed to a Federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

d. *Congressional inquiries disclosure routine use.* Disclosure from an Army system of records may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual. This does not authorize the disclosure of a record without the consent of the individual.

e. *Private Relief Legislation routine use.* Relevant information contained in all DOD systems of records published on or before August 22, 1975, will be disclosed to the OMB in connection with the review of private relief legislation as set

forth in OMB Circular A-19, at any stage of the legislative coordination and clearance process as set forth in that circular.

*f. Disclosures required by international agreements routine use.* A record from an Army system of records may be disclosed to foreign law enforcement, security, investigatory, or administrative authorities to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements including those regulating the stationing and status in foreign countries of DOD military and civilian personnel.

*g. Disclosures to State and local taxing authorities routine use.* Any information normally contained in Internal Revenue Service Form W-2 (Wage and Tax Statement), which is maintained in a record from an Army system of records, may be disclosed to State and local taxing authorities where the Secretary of the Treasury has entered into agreements under 5 USC 5516, 5517, and 5520, and only to those state and local taxing authorities for which an employee or military member is or was subject to tax regardless of whether tax is or was withheld. This routine use complies with Treasury Fiscal Requirements Manual, Bulletin No. 76-07.

*h. Disclosures to Office of Personnel Management routine use.* A record from an Army system of records subject to the Privacy Act and maintained by a DA activity may be disclosed to the OPM concerning information on pay and leave, benefits, retirement deductions, and any other information necessary for OPM to carry out its legally authorized Government-wide personnel management functions and studies.

*i. Disclosures to the Department of Justice for litigation routine use.* A record from an Army system of records may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing DOD, or any officer, employee, or member of DOD in pending or potential litigation where the record is pertinent.

*j. Disclosures to military banking facilities overseas routine use.* Information as to current military addresses and assignments may be provided to military banking facilities providing banking services to military members assigned overseas when those banks are reimbursed by the Government for certain checking and loan losses. For personnel separated, discharged, or retired from the armed services, information as to last known residential or home of record address may be provided to the military banking facility upon certification by a banking facility officer that the facility has a returned or dishonored check negotiated by DOD personnel or contractors or the individual has defaulted on a loan and that if restitution is not made by the individual, the U.S. Government will be liable for the losses the bank may incur.

*k. Disclosures to the General Services Administration routine use.* A record from an Army system of records may be disclosed as a routine use to GSA for the purpose of records management inspections conducted under authority of 44 USC 2904 and 44 USC 2906.

*l. Disclosures of Information to the National Archives and Records Administration routine use.* A record from an Army system of records may be disclosed as a routine use to National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 USC 2904 and 44 USC 2906.

*m. Disclosures to the Merit Systems Protection Board routine use.* A record from an Army system of records may be disclosed as a routine use to the Merit Systems Protection Board, the Office of the Special Counsel for the purpose of litigation, including administrative procedures, appeals, special studies of the civil service and other merit systems, review of Office of Personnel Management or component rules and regulations, investigation of alleged or possible prohibited personnel practices, including administrative proceedings involving any individual subject of a DOD investigation, and such other functions, promulgated in 5 USC 1205 and 5 USC 1206, or as may be authorized by law.

*n. Disclosures for counterintelligence purposes.* A record from an Army system of records may be disclosed as a routine use outside the DOD or the U.S. Government for the purpose of counterintelligence activities authorized by U.S. law or executive order or for the purpose of enforcing laws, which protect the national security of the United States.

*o. Disclosures for data breach remediation purposes.* A record from an Army system of records may be disclosed to appropriate agencies, entities, and persons when the following conditions are met:

(1) The component suspects or has confirmed that the security or confidentiality of the information in the system of records has been compromised;

(2) The component has determined that as a result of the suspected or confirmed compromise a risk exists of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the component or another agency or entity) that rely upon the compromised information; and

(3) The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the component's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

*p. Information sharing environment.* A record from an Army system of records consisting of, or relating to, terrorism information (6 USC 485(a)(4)), homeland security information (6 USC 482(f)(1)), or law enforcement information (Guideline 2 Report attached to White House Memorandum, "Information Sharing Environment," November 22, 2006) may be disclosed to a Federal, State, local, tribal, territorial, foreign governmental, and/or multinational agency, either in

response to its request or upon the initiative of the Army, for purposes of sharing as necessary and relevant for the agencies to the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America as contemplated by the Intelligence Reform and Terrorism Protection Act of 2004 (Public Law 108-458) and Executive Order 13388.

### **3-4. Computer matching**

*a.* The Computer Matching and Privacy Protection Act of 1988 amends the Privacy Act of 1974 to establish procedural safeguards affecting agencies use of Privacy Act records in performing certain types of computerized programs.

*b.* The Privacy Act applies to matching programs that use records from Federal personnel or payroll systems and Federal benefit programs where matching meets the following criteria:

- (1) Determines eligibility for federal benefit;
- (2) Determines compliance with benefit program requirements; or
- (3) Recovers improper payments or delinquent debts from current or former beneficiaries.

*c.* The comparison of records must be computerized; manual comparisons do not apply.

*d.* In all cases, Computer Matching Agreements are processed by the DPCLD as specified in DOD 5400.11-R and approved by the Defense Data Integrity Board. The Chief, DA FOIA/PA is a member of the Defense Data Integrity Board. Agreements are conducted in accordance with the requirements of 5 USC 552a and OMB Circular A-130. For additional information regarding the computer matching publication and review requirements, see DOD 5400.11-R.

## **Chapter 4 Exemptions**

### **4-1. Exempting systems of records**

The Secretary of the Army, or a designee, may exempt Army systems of records from certain requirements of the Privacy Act under the following provisions:

*a.* General exemption (j)(2)—Relieves systems of records from most requirements of the Privacy Act. Only Army activities actually engaged in the enforcement of criminal laws as their primary function may claim this exemption.

*b.* Specific exemptions (k)(1) – (k)(7)—Relieves systems of records from a few selected provisions of the Act.

*c.* Access exemption (d5)—Relieves systems of records from the access provision of the Privacy Act. This exemption applies to information compiled in reasonable anticipation of a civil action or proceeding.

### **4-2. General exemption**

Only Army activities actually engaged in the enforcement of criminal laws as their principal function may claim the general exemption. To qualify for this exemption, a system must consist of—

*a.* Information compiled to identify individual criminals and alleged criminals, which consists only of identifying data and arrest records; type and disposition of charges; sentencing, confinement, and release records; and parole and probation status.

*b.* Information compiled for the purpose of a criminal investigation, including efforts to prevent, reduce, or control crime, and reports of informants and investigators associated with an identifiable individual.

*c.* Reports identifiable to an individual, compiled at any stage of the process of enforcement of the criminal laws, from arrest or indictment through release from supervision.

### **4-3. Specific exemptions**

The Secretary of the Army has exempted from certain parts of the Privacy Act all properly classified information and a few systems of records that have specific categories of information. The Privacy Act exemption cited appears in brackets after each category.

*a.* *Classified information in every Army system of records.* Before denying an individual access to classified information, the Denial Authority must make sure that it was properly classified under the standards of Executive Order 11652 or 12356 and that it must remain classified in the interest of National defense or foreign policy. [5 USC 552a(k)(1)]

*b.* *Investigatory data for law enforcement purposes (other than that claimed under the general exemption).* However, if this information has been used to deny someone a right, privilege, or benefit to which the individual is entitled by Federal law, it must be released, unless doing so would reveal the identity of a confidential source. [5 USC 552a(k)(2)]

*c.* *Records connected to protective services.* Records maintained in connection with providing protective services to the President of the United States or other individuals protected based on 18 USC 3056 (5 USC 552a(k)(3)).

*d. Statistical data.* Statistical data required by statute and used only for statistical purposes and not to make decisions on the rights, benefits, or entitlements of individuals, except for census records that may be disclosed under 13 USC 8. [5 USC 552a(k)(4)]

*e. Federal service data.* Data compiled to determine suitability, eligibility, or qualifications for Federal service, Federal contracts, or access to classified information. This information may be withheld only to the extent that disclosure would reveal the identity of a confidential source. [5 USC 552a(k)(5)]

*f. Federal service testing material.* Testing material used to determine if a person is qualified for appointment or promotion in the Federal service. This information may be withheld only if disclosure would compromise the objectivity or fairness of the examination process. [5 USC 552a(k)(6)]

*g. Information to determine promotion potential in the Armed Forces.* Information may be withheld, but only to the extent that disclosure would reveal the identity of a confidential source. [5 USC 552a(k)(7)]

#### **4-4. Army systems of records notices citing exemptions**

*a.* When a system manager seeks an exemption for a system of records, the following information should be furnished to the Army Privacy Office:

- (1) Applicable system notice.
- (2) Exemptions sought.
- (3) Justification.

*b.* After appropriate staffing and approval by the Secretary of the Army, or delegated representative, the rule is forwarded to DPCLD for publication in the Federal Register. No exemption may be invoked until these steps have been completed. See appendix C for a listing of the Army system of record notices (SORNs) citing exemptions. For the most current listing of Army SORNs, see the Records Management and Declassification Agency (RMDA) Web site: <https://www.rmda.army.mil/privacy/sorns/armypublishedsorn.html>.

## **Chapter 5**

### **Handling and Safeguarding Personally Identifiable Information**

#### **5-1. Collecting personally identifiable information**

*a.* When collecting PII, Army administrators and other users of PII must observe the provisions and guidelines described in this section. This section applies to Army military and civilian personnel and Government contractors.

*b.* General provisions for collecting PII are as follows:

(1) The Army collects PII directly from the subject of the record whenever possible. This is especially important when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs.

(2) When an Army activity asks an individual for his or her PII that will be maintained in a system of records, the Activity must provide the individual with a PAS. A PAS notifies individuals of the authority, purpose, and use of the collection, whether the information is mandatory or voluntary, and the effects of not providing all or any part of the requested information. See paragraph 5-3 when soliciting SSNs for any purpose.

*c.* A PAS must be prepared and administered based on the following guidelines:

- (1) The Federal statute or executive order that authorizes collection of the requested information.
- (2) The principal purpose or purposes for which the information is to be used.
- (3) The routine uses that will be made of the information.
- (4) Whether providing the information is voluntary or mandatory.
- (5) The PAS includes language that is explicit, easily understood, and concise.
- (6) A sign is displayed in areas where people routinely furnish this kind of information, and a copy of the PAS is made available upon request by the individual.
- (7) The individual reads, but does not sign the PAS.
- (8) A PAS must include the following items:
  - (a) Authority:* Cite the specific statute or executive order, including a brief title or subject that authorizes the DA to collect the PII requested.

*(b) Principal purposes:* Cite the principal purposes for which the information will be used.

*(c) Routine uses:* Cite the routine uses for which the information may be used. This may be a summary of information published in the applicable system of records notice. Applicable routine uses are published in the applicable Privacy Act system of records notice. If none, the language to be used is: "Routine Use: None. However the 'Blanket Routine Uses' set forth at the beginning of the Army's compilation of systems of records notices may apply."

*(d) Disclosure: Voluntary or Mandatory.* Include in the PAS specifically whether furnishing the requested PII is voluntary or mandatory. A requirement to furnish PII is mandatory only when a Federal statute, executive order, regulation, or other law specifically imposes a duty on the individual to provide the information sought, and when the individual is subject to a penalty if he or she fails to provide the requested information. If providing the information is only a condition of or prerequisite to granting a benefit or privilege and the individual has the option of requesting that benefit, then the collection is voluntary. However, the loss or denial of the privilege, benefit, or entitlement sought must be listed as a consequence of not furnishing the requested information.

*d.* Some acceptable means of administering the PAS are as follows, in the order of preference:

(1) Below the title of the media used to collect the PII (positioning the PAS so the individual will observe the PAS before providing the requested information).

(2) Within the body with a notation of its location below the title.

(3) On the reverse side with a notation of its location below the title.

(4) Attached as a tear-off sheet.

(5) Issued as a separate supplement.

*e.* The usage and elements of a PAS are described in appendix D.

*f.* Include a PAS on a Web site if the site requires information directly from an individual and the information is retrieved by his or her name or personal identifier.

*g.* When collecting PII from third parties, it may not be practical to collect personal information directly from the individual in all cases. Some examples of when third-party collection may be necessary include—

(1) To verify information.

(2) To solicit opinions or evaluations.

(3) To use another source when the subject cannot be contacted.

(4) At the request of the subject individual.

*h.* When asking third parties to provide information about other individuals, advise them of—

(1) The purpose of the request.

(2) Their rights to confidentiality as defined by the Privacy Act.

*Note.* Consult with your servicing Staff Judge Advocate for potential limitations to the confidentiality that may be offered.

*i.* Promises of confidentiality must be prominently annotated in the record to protect from disclosing any information provided in confidence based on 5 USC 552a(k)(2), (k)(5), or (k)(7).

## **5-2. Safeguarding personally identifiable information**

*a.* The Privacy Act requires establishment of proper administrative, technical, and physical safeguards to—

(1) Ensure the security and confidentiality of records (for example, to periodically verify that only personnel with a current and valid need to know have access to shared drives and document management systems).

(2) Protect against any threats or hazards to the subject's security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness.

*b.* At each location, and for each system of records, an official will be designated to safeguard the information in that system. Consideration must be given to such items as sensitivity of the data, need for accuracy and reliability in operations, general security of the area, and cost of safeguards. (See AR 25-2.)

*c.* Ordinarily, PII must be afforded at least the protection required for information designated "For Official Use Only." Privacy Act data will be afforded reasonable safeguards to prevent inadvertent or unauthorized disclosure of record content during processing, storage, transmission, and disposal.

*d.* With the growing use of Web sites, the proliferation of social media, and the increasing risks of and cases of identity theft, the dimensions for the safeguarding of data have expanded exponentially in recent decades. Web masters and Web maintainers must apply appropriate privacy and security policies to respect user privacy. As specified in AR 25-1, organizations must screen their Web sites and display a privacy and security notice in a prominent location on at least the first page of all major sections of each Web site. Each Web site must clearly and concisely inform visitors to the site about any information the activity collects, why it is collected, and how it will be used.

*e.* Each privacy and security notice must clearly and concisely inform visitors to the site what information the activity collects about individuals, why it is collected, and how it will be used. If PII is requested in the notification and record access procedures, but not collected or listed in the categories of records, the reason for requesting the PII must be explained.

*f.* If the SSN is used for verification purposes, the custodian of the record must state "SSN required for verification purposes only."

g. The DA recognizes the importance of safeguarding PII in all forms of electronic media in addition to paper media. For information on approved Army use of social media, see Web site: <http://www.army.mil/mobile/socialmedia.html>.

### **5–3. Protecting social security numbers**

a. When soliciting or using SSNs, Army administrators and other users of SSNs observe the provisions and guidelines described in this section. It is unlawful for any Federal, State, or local Government agency to deny anyone a legal right, benefit, or privilege provided by law for refusing to give their SSN unless the law requires disclosure, or a law or regulation adopted before January 1, 1975, required the SSN or if DA uses the SSN to verify a person's identity in a system of records established and in use before that date. Executive Order 9397 (issued prior to January 1, 1975) authorizes the Army to solicit and use the SSN as a numerical identifier for individuals in most federal records systems. However, the SSN should only be collected as needed to perform official duties. EO 9397 does not mandate the solicitation of SSNs from Army personnel as a means of identification.

b. Upon entrance into military service or civilian employment with DA, individuals are asked to provide their SSN. The SSN becomes the service or employment number for the individual and is used to establish personnel, financial, medical, and other official records. After an individual has provided his or her SSN for the purpose of establishing a record, the PAS is not required if the individual is only requested to furnish or verify the SSN for identification purposes in connection with the normal use of his or her records. If the SSN is to be used for a purpose other than identification, the individual must be informed whether disclosure of the SSN is mandatory or voluntary; by what statutory authority the SSN is solicited; and what uses will be made of the SSN. This notification is required even if the SSN is not to be maintained in a Privacy Act system of records.

c. The current use of the Department of Defense ID (DOD ID) number is gradually replacing use of the SSN. Increased use of the DOD ID helps to minimize use of the SSN and assists with the safeguarding process.

d. Only those records covered by a Privacy Act SORN may be arranged to permit retrieval by a personal identifier (for example, an individual's name or SSN). AR 25–400–2 requires all records covered by a Privacy Act system of records notice to include the system of record identification number on the record label to serve as a reminder that the information contained within must be safeguarded.

## **Chapter 6 Individual Access to Records and Denials**

### **6–1. Individual access applicability**

The Privacy Act's access provision permits an individual to gain access to "his or her record or to any information pertaining to him or her" that is contained in a system of records indexed and retrieved by their name or personal identifier. [5 USC 552a(d)(1)]

a. Upon a written request, an individual will be granted access to information pertaining to him or her that is maintained in a Privacy Act system of records, except in the following conditions:

- (1) The information is subject to an exemption, and the system manager has invoked the exemption.
- (2) The information is compiled in reasonable anticipation of a civil action or proceeding.

b. Legal guardians or parents acting on behalf of a minor child have the rights of access under the Privacy Act, unless the records were created or maintained during circumstances where the interests of the minor child were adverse to the interests of the legal guardian or parent.

c. These provisions should allow for the maximum release of information consistent with Army and DOD statutory responsibilities.

*Note.* Privacy Act requests can be made only by requesters asking for information within a system of records concerning themselves, their minor children, and persons for whom legal guardianship has been established. (A minor is an individual under 18 years of age, who is not a member of the U.S. Army, or married. Minors of interest to this regulation are usually children or legal dependents of U.S. Army members; dependents are not necessarily minors.)

### **6–2. Individual requests for access**

Individuals must submit requests for access to records in a Privacy Act system of records to the system manager or the custodian of the record designated in DA SORNs. For the most current listing of Army SORNs, see the Records Management and Declassification Agency (RMDA) Web site: <https://www.rmda.army.mil/privacy/sorns/armypublishedsorn.html>.

a. Individual requests for record access must be submitted in writing.

b. Individuals do not have to state a reason or justify the need to gain access to records under the Privacy Act. However, requesters should reasonably describe the records they are requesting.

c. Before granting access to personal data, an individual must provide verification of identity (for example, submission of a notarized signature). An alternative method for verifying identity is an un-sworn declaration in accordance with 28 USC 1746 in the following format:

(1) If executed within the United States, its territories, possessions, or commonwealths: “I declare under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).”

(2) If executed outside of the United States: “I declare under perjury or penalty under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).”

d. If an individual seeks access in person, identification can be verified by a Government-issued identification card, driver’s license, or other license, permit, or pass normally used for identification purposes.

e. If an individual wishes to have their records released directly to a third party or to be accompanied by a third party when seeking access to their records, reasonable proof of authorization must be obtained. The individual must furnish a signed access authorization with a notarized signature before granting the third party access.

### **6–3. Individual access to medical records**

a. Access to medical records is not only governed by the access provisions of this regulation, but also by the access provisions of DOD 6025.18–R. The Privacy Act, as implemented by this regulation, however, provides greater access to an individual’s medical records than that authorized by DOD 6025.18–R.

b. Medical records in a system of records will be disclosed to the individual to whom they pertain, even if a minor; but, when it is believed that access to such records could have an adverse effect on the mental or physical health of the individual or may result in harm to a third party, the following special procedures apply:

(1) If a determination is made in consultation with a medical doctor that release of the medical information may be harmful to the mental or physical health of the individual, or to a third party, the Army activity will—

(a) Send the record to a physician named by the individual; and

(b) Explain why access by the individual without proper professional supervision could be harmful (unless it is obvious from the record), in the transmittal letter to the physician.

(2) Army activities shall not require the physician to request the records for the individual.

c. If the individual refuses or fails to designate a physician, the record shall not be provided. Such refusal of access is not considered a denial under the Privacy Act.

d. If records are provided to the designated physician, but the physician declines or refuses to provide the records to the individual, the Army activity is under an affirmative duty to take action to deliver the records to the individual by whatever means deemed appropriate. Such action should be taken expeditiously, especially after a significant delay between when the records were furnished the physician and the decision by the physician not to release the records.

e. Access to a minor’s medical records may be granted to their parents or legal guardians. However, access is subject to the restrictions as set forth in DOD 6025.18–R.

f. Members of the Army and all married persons are not considered minors regardless of age, and the parents of these individuals do not have access to their medical records without written consent of the individual.

### **6–4. Personal notes**

a. The Privacy Act does not apply to personal notes of individuals used as memory aids. These documents are not considered Privacy Act records. The five conditions for documents to be considered as personal notes of individuals used as memory aids are as follows:

(1) Maintained and discarded solely at the discretion of the author,

(2) Created only for the author’s personal convenience and restricted to that of memory aids,

(3) Not the result of official direction or encouragement, whether oral or written,

(4) Not shown to others for any reason, and

(5) Not filed in agency files.

b. Any disclosure from personal notes, either intentional or unintentional, removes the information from the category of memory aids and the personal notes then become subject to provisions of the Privacy Act.

### **6–5. Relationship between Privacy Act and Freedom of Information Act**

Not all requesters are knowledgeable of the appropriate statutory authority to cite when requesting records. In some instances, they may cite neither the Privacy Act nor the FOIA, but will imply one or both Acts. The guidelines below are provided to ensure that requesters are given the maximum amount of information as authorized under both statutes.

a. Privacy Act requests can be made only by those asking for information within a system of records concerning themselves, persons for whom legal guardianship has been established, and for parents of minor children. Unlike FOIA, the Privacy Act applies only to U.S. citizens and aliens lawfully admitted for permanent residence.

*b.* Requests for individual access will be processed as follows:

(1) If the records are required to be released in accordance with the Privacy Act, FOIA does not bar release even if a FOIA exemption could be invoked if the request had been processed solely pursuant to FOIA. Conversely, if the records are required to be released pursuant to FOIA, the Privacy Act does not bar disclosure.

(2) Requesters who seek records about themselves contained in a system of records, and who cite or imply only the Privacy Act, will have their records processed in accordance with the provisions of the Privacy Act and the FOIA. If the system of records is exempt from the access provisions of the Privacy Act, and if the records, or any portion thereof, are exempt pursuant to FOIA, the requester should be advised and informed of the applicable Privacy and FOIA exemptions. Only in cases where the records can be denied in accordance with both statutes may the Army withhold the records from the individual. Appeals will be processed in accordance with provisions of both the Privacy Act and FOIA.

(3) Requesters who seek records about themselves that are not contained in a system of records, and who cite or imply only the Privacy Act, will have their requests processed in accordance with the provisions of AR 25–55, since the access provisions of the Privacy Act do not apply. Appeals will be processed in accordance with the provisions of FOIA.

(4) An individual's access to PII concerning themselves, which would otherwise be releasable to them in accordance with either The Privacy Act or FOIA will not be denied solely because they fail to cite or imply either the Privacy Act, FOIA, or cite the wrong act, regulation, manual, or instruction.

## **6–6. Denial authorities**

*a.* The only officials authorized to deny a request for records or a request to amend records in a PA system of records are the appropriate denial authorities, their designees, or the Secretary of the Army, acting through the General Counsel.

*b.* Denial authorities are authorized to deny requests, either in whole or in part, for access and amendment of Privacy Act records contained in their respective areas of responsibility. The following denial procedures must be followed:

(1) The denial authority may delegate complete or partial decision authority to a division chief under his or her supervision within the Army activity in the grade of O–5/GS–14 or higher. All delegations must be in writing.

(2) The denial authority will send the names, office names, and telephone numbers of their delegates to the DA Freedom of Information and Privacy Office.

(3) If a denial authority delegate denies access or amendment, the delegate must clearly state that he or she is acting on behalf of the denial authority, who must be identified by name and position in the written response to the requester. Denial authority designation will not delay processing privacy requests/actions.

(4) The official denial authorities are for records under their authority (see app B). The individuals designated as denial authorities under this regulation are often the same individuals designated as Initial Denial Authorities under AR 25–55.

(5) The custodian of the record will acknowledge requests for access made under the provisions of the Privacy Act within 10 working days of receipt.

(6) The custodian will forward requests for information recommended for denial to the appropriate denial authority, along with a copy of the request, disputed records, and justification for withholding the information.

(7) Within 30 working days, the denial authority will provide the following notification to the requester in writing if the decision is to deny the requester access to the information:

*(a)* Denying official's name, position title, and business address.

*(b)* Date of the denial.

*(c)* Reasons for the denial, including citation of the appropriate subsections of the Privacy Act and this regulation.

*(d)* The individual's right to administratively appeal the denial within 60 calendar days of the mailing date of the notice, through the denial authority, to the Office of the General Counsel, Secretary of the Army, 104 Army Pentagon, Washington, DC 20310–0104.

(8) The appeal must be in writing and the requester should provide a copy of the denial letter and a statement of reasons for seeking review. For denials made by the DA when the record is maintained in a Government-wide system of records, an individual's request for further review must be addressed to each of the appropriate Government Privacy Act offices listed in the Privacy Act system of records notices. For a current listing of Government-wide Privacy Act system of records notices see the DPCLD Web site: [http://dpclд.defense.gov/privacy/sornsindex/governmentwidenotices.aspx](http://dpclد.defense.gov/privacy/sornsindex/governmentwidenotices.aspx).

(9) Denial is appropriate only if the record meets either of the following conditions:

*(a)* Was compiled in reasonable anticipation of a civil action or proceeding.

*(b)* Is exempted by the Secretary of the Army from the disclosure provisions of the Privacy Act, a legitimate governmental purpose for invoking the exemption exists, and the record is not required to be disclosed under the Freedom of Information Act.

*c.* Once the Army General Counsel issues a determination, the requester has the right to contest the decision within the U.S. District Court of the appropriate jurisdiction. The case is then forwarded to the Litigation Division, OTJAG.

## 6–7. Fees

Requesters will be charged only for reproduction of requested documents. Normally, there will be no charge for the first copy of a record provided to an individual to whom the record pertains. Thereafter, fees will be computed as set forth in AR 25–55.

## Chapter 7

### Disclosure of personal records to other agencies and third parties

#### 7–1. Disclosure to third parties

The Army is limited from disclosing a record from a system of records without obtaining the prior written consent of the individual, except when disclosure is—

*a. Made to officers and employees of DOD who have a need for the record in the performance of their duties.* For the purpose of disclosures and accounting of disclosures, DOD is considered a single agency, therefore, disclosures within Army activities and other DOD components are not considered third party requests, and the requirements for consent for disclosure and disclosure accounting do not apply.

*b. Required under the Freedom of Information Act.* The FOIA requires that records be made available to the public unless withholding is authorized pursuant to one of nine exemptions or one of three law enforcement exclusions under the Act. (See AR 25–55 for additional information.)

(1) Army activities must be in receipt of a FOIA request and a determination made that the records are not withholdable pursuant to a FOIA exemption or exclusion before records may be disclosed.

(2) Records that have traditionally been held to be in the public domain or which are required to be disclosed to the public, such as press releases, may be disclosed independent of a FOIA request.

*c. Protected by Freedom of Information Act provisions.* Personal privacy interests are protected by two provisions of the FOIA, exemptions 6 and 7(C). FOIA exemption 6 applies to most personal records, such as personnel, medical, and similar records. Exemption 7(C) applies to personal records compiled for law enforcement purposes, including personnel security investigation records. Both exemptions apply when disclosure of information would constitute a clearly unwarranted invasion of personal privacy.

(1) Disclosures of personal information regarding military and civilian employees should be made in accordance with the following considerations:

*(a)* Lists or compilations of unit or office address or telephone numbers are not released where the requester’s primary purpose in seeking the information is to use it for commercial solicitation.

*(b)* Listings of personnel currently or recently assigned, details, or employed with the Army are not releasable if the disclosure of such a list would pose a privacy or security threat.

*(c)* Information regarding military or civilian personnel assigned, detailed, or employed by the National Security Agency, the Defense Intelligence Agency, the National Reconnaissance Office, or the National Geospatial-Intelligence Agency, may only be disclosed as authorized by Public Law 86-36 (1959) and 10 USC 424 information pertaining to personnel assigned, detailed, or employed by an overseas unit, a sensitive unit can be withheld from disclosure under 10 USC 130b.

(2) Military personnel information that may be disclosed under the FOIA includes—

*(a)* Name.

*(b)* Rank.

*(c)* Date of rank.

*(d)* Gross salary.

*(e)* Past and present duty assignments.

*(f)* Future continental United States (CONUS) assignments that are officially established.

*(g)* Office/unit name, duties address, and telephone number.

*(h)* Source of commission, promotion sequence number, military awards and decorations, and military and civilian education.

*(i)* Duty status, at any given time.

*(j)* Separation or retirement dates.

*(k)* Biographies and photos of key personnel.

(3) Civilian employee information that may be disclosed under the Freedom of Information Act includes—

*(a)* Name.

*(b)* Past and present position titles, occupational series, and grade.

*(c)* Past and present annual salary rates (including performance awards or bonuses, incentive awards, merit pay amount, Meritorious or Distinguished Executive Ranks, and allowances and differentials).

- (d) Past and present duty stations.
- (e) Office or duty telephone number.
- (4) In addition to the disclosure of information regarding civilian employees, the following information may be made available to a prospective employer of a current or former Army employee:
  - (a) Tenure of employment.
  - (b) Civil service status.
  - (c) Length of service in the Army and the Government.
  - (d) Date and reason for separation shown on Standard Form (SF)–50 (Notification of Personnel Action).
- (5) Disclosure of personal information regarding Army civilian personnel must be made in accordance with OPM policies.
- (6) Nonappropriated funds employee personal information that may be disclosed under the Freedom of Information Act includes—
  - (a) Name.
  - (b) Grade, date, or position.
  - (c) Gross salary.
  - (d) Past and present duty assignments.
  - (e) Future assignments, if officially established.
- (7) Information permitted by a routine use that has been published in the Federal Register:
  - (a) Made to the Bureau of the Census for planning or carrying out a census or survey, or to a related activity pursuant to Title 13 of the United States Code.
  - (b) Made to a recipient who has provided the Army with advance written assurance that the records will be—
    1. Used solely as a statistical research or reporting record.
    2. Transferred in a form that is not individually identifiable.
  - (c) Made to the National Archives of the United States as a record that has sufficient historical or other value to warrant its continued preservation by the U.S. Government, or for determination of such value by the Administrator of the General Services Administration (GSA), or designee. (Records sent to Federal Records Centers for storage remain under Army control. These transfers are not disclosures and do not therefore need an accounting.)
  - (d) Made to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if—
    1. The activity is authorized by law.
    2. The head of the agency or instrumentality has made a written request to the Army element that maintains the record. The request must specify the particular portion desired and the law enforcement activity for which the record is sought.
  - (e) Made to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual. Upon such disclosure notification will be transmitted to the last known address of such individual.
  - (f) Made to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress, or subcommittee of any such joint committee.
  - (g) Made to the Comptroller General, or authorized representatives, in the course of the performance of the duties of the General Accounting Office (GAO).
  - (h) Pursuant to the order signed by a judge of a court of competent jurisdiction. (Reasonable efforts must be made to notify the subject individual if the legal process is a matter of public record.)
  - (i) Made to a consumer reporting agency under section 3(d) of the Federal Claims Collection Act of 1966 (implemented by 49 CFR part 89). The name, address, SSN, and other information identifying the individual; amount, status, and history of the claim; and the agency or program under which the case arose may be disclosed in this instance.

## **7–2. Disclosure accounting**

- a. An accounting of disclosure is required whenever a record from an Army system of records is disclosed to someone other than the data subject, except when records are—
  - (1) Disclosed to DOD officials who have a “need to know” the information to perform official Government duties.
  - (2) Required to be disclosed under the Freedom of Information Act.
- b. Since the characteristics of records maintained within DA vary widely, no uniform method for keeping the disclosure accounting is prescribed.
- c. Essential elements to include in each disclosure accounting report are—
  - (1) The name, position title, and address of the person making the disclosure.
  - (2) Description of the record disclosed.
  - (3) The date, method, and purpose of the disclosure.

- (4) The name, position title, and address of the person or agency to which the disclosure was made.
- d.* The purpose for the accounting of disclosure is to—
  - (1) Enable an individual to ascertain those persons or agencies that have received information about them.
  - (2) Enable the DA to notify past recipients of subsequent amendments or “Statements of Dispute” concerning the record.
  - (3) Provide a record of DA compliance with the Privacy Act of 1974, if necessary.
- e.* When an individual requests such an accounting, the system manager or designee will respond within 20 workdays and inform the individual of the items above.
- f.* The only bases for not furnishing the data subject an accounting of disclosures are if disclosure was made for law enforcement purposes under 5 USC 552a(b)(7), or the disclosure was from a system of records for which an exemption from 5 USC 552a(c)(3) has been claimed.
- g.* There are no approved filing procedures for the disclosure of accounting records; however, system managers must be able to retrieve them upon request. With this said, disclosure accountings should be kept for 5 years after the disclosure, or for the life of the record, whichever is longer.

## **Chapter 8**

### **Amending Records and Department of the Army Privacy Act Review Board**

#### **8–1. Periodic review and amendment of records**

- a.* Individuals are encouraged to periodically review the information maintained about them in Privacy Act systems of records and to familiarize themselves with the amendment procedures established by this regulation.
- b.* An individual may request to amend records that are retrieved by his or her name or personal identifier from a system of records unless the system has been exempted from the amendment provisions of the Act. The standard for amendment is that the records are inaccurate as a matter of fact rather than judgment, irrelevant, untimely, or incomplete. The burden of proof is on the requester.
- c.* The system manager or custodian must review Privacy Act records for accuracy, relevance, timeliness, and completeness.
- d.* Amendment procedures are not intended to permit individuals to challenge events in records that have actually occurred. Amendment procedures only allow individuals to amend those items that are factually inaccurate and not matters of official judgment (for example, performance ratings, promotion potential, and job performance appraisals). In addition, an individual is not permitted to amend records for events that have been the subject of judicial or quasi-judicial actions and/or proceedings.
- e.* An amendment does not allow an individual to challenge the merits of an adverse action. However, if the record contains a misspelled name or an incorrect date of birth or SSN, the amendment procedures may be used to request correction of the record.
- f.* USACIDC reports of investigations have been exempted from the amendment provisions of the Privacy Act. Requests to amend these reports will be considered under AR 195–2 by the Commander, U.S. Army Criminal Investigation Command. Actions by the Commander of U.S. Army Criminal Investigation Command will constitute final action on behalf of the Secretary of the Army under that regulation.
- g.* Inspector General investigative files and action/request/complaint files (records in system notice A0021-1 SAIG, Inspector General Records) have been exempted from the amendment provisions of the Privacy Act. Requests to amend these reports will be considered under AR 20-1 by the Inspector General. Action by the Inspector General will constitute final action on behalf of the Secretary of the Army under that regulation.
- h.* Records placed in the National Archives are exempt from the Privacy Act provision allowing individuals to request amendment of records. Most provisions of the Privacy Act apply only to those systems of records that are under the legal control of the originating agency; for example, an agency’s current operating files or records stored at a Federal Records Center.
- i.* Amendment procedures are as follows:
  - (1) Requests to amend records should be addressed to the custodian or system manager of the records. The request must reasonably describe the records to be amended and the changes sought (for example, deletion, addition, or amendment). The burden of proof is on the requester.
  - (2) The system manager or records custodian will provide the individual with a written acknowledgment of the request within 10 working days and will make a final response within 30 working days of the date the request was received. The acknowledgment must clearly identify the request and inform the individual that final action will be forthcoming within 30 working days.

(3) Records for which amendment is sought must be reviewed by the proper system manager or custodian for accuracy, relevance, timeliness, and completeness to ensure fairness to the individual in any determination made about that individual on the basis of that record.

(4) If the amendment is appropriate, the system manager or custodian will physically amend the records accordingly. The requester will be notified of such action.

(5) If the amendment is not warranted, the request and all relevant documents, including reasons for not amending, will be forwarded to the proper denial authority within 10 working days to ensure that the 30-day time limit for the final response is met. In addition, the requester will be notified of the referral.

(6) Based on the documentation provided, the denial authority will either amend the records and notify the requester and the custodian of the records of all actions taken, or deny the request. If the records are amended, those who have received the records in the past will receive notice of the amendment.

(7) If the denial authority determines that the amendment is not warranted, he or she will provide the requester and the custodian of the records reason(s) for not amending. In addition, the denial authority will send the requester an explanation regarding his or her right to seek further review by the DA Privacy Act Review Board, through the denial authority, and the right to file a concise "Statement of Disagreement" to append to the individual's records.

### **8-2. Department of the Army Privacy Act Review Board appeal process**

*a.* The DA Privacy Act Review Board acts on behalf of the Secretary of the Army in deciding appeals of the appropriate denial authority's refusal to amend records. The Board will process an appeal within 30 working days of its receipt. The General Counsel may authorize an additional 30 days when unusual circumstances and good cause so warrant. The Board may seek additional information, including the appellant's official personnel file, if relevant and necessary to decide the appeal. The Board membership consists of the following principal members, with three voting and two non-voting members, or their delegates:

*b.* The voting members of the Board are representatives of the AASA, the Army Privacy Office, and The Judge Advocate General. The denial authority may send a representative to the Board when a case within its purview is discussed; however, the representative is a nonvoting member and he or she may only be present when the specific applicable case is discussed.

*c.* The two nonvoting members are—

(1) Chief Attorney, OAASA serves as the legal advisor and will be present (or send a designee) for all Board sessions.

(2) Recording Secretary provided by the Army Privacy Office.

### **8-3. Department of the Army Privacy Act Review Board meetings**

The DA Privacy Act Review Board holds meetings based on the following requirements:

*a.* The meeting of the Board requires the presence of all five members or their designated representatives. Other non-voting members, all of whom will be either full-time or permanent part-time employees of the Federal Government, with subject matter expertise may participate in a meeting of the Board, at the discretion of the Chairperson. Participation can be either physical or by telecommunications.

*b.* Majority vote of the voting members is required to make a final determination on a request before the Board.

*c.* The Board may seek additional information, including the requester's official personnel file, if relevant and necessary to decide the appeal.

*d.* If the Board determines that an amendment is justified the Board will amend the record and notify the requester, the denial authority, the custodian of the record, and any prior recipients of the record, of the amendment.

*e.* If the Board determines that amendment is unwarranted, it will—

(1) Obtain the General Counsel's concurrence in writing.

(2) Respond to the requester with the reasons for denial.

(3) Inform the requester of the right to file a "Statement of Disagreement" with the Board's action and to seek judicial review of the Army's refusal to amend. A "Statement of Disagreement" must be received by the system manager within 120 days and it will be made an integral part of the pertinent record. Anyone who may have access to, use of, or need to disclose information from the record will be aware that the record has been disputed. The disclosing authority may include a brief summary of the Board's reasons for not amending the disputed record.

*f.* It is inappropriate for the DA Privacy Act Review Board to consider any record which is exempt from the amendment provision of the Privacy Act.

## Chapter 9 Breach Reporting, Risk Assessment, Notification, and Mitigation

### 9–1. Breach process

For the purpose of safeguarding against and responding to the breach of PII, the term “breach” is used to include the 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. A breach/compromise incident occurs when it is suspected or confirmed that PII is lost, stolen, improperly disclosed or otherwise available to individual(s) without a duty related official need to know. When reporting an actual or suspected breach heads of Army Staff agencies, ACOMs, ASCCs, and DRUs are responsible for reporting any actual or suspected compromises of PII within their activity. Army activities should report all incidents involving PII in physical or electronic form and should not distinguish between suspected and confirmed breaches. Reporting considerations are—

*a.* Report all cyber related incidents involving the actual or suspected breach/compromise of PII within one hour of discovery to the United States Computer Emergency Readiness Team (US-CERT) by entering a report into the US-CERT Incident Reporting System at <https://www.us-cert.gov/forms/report> or to US-CERT at (888) 282–0870 (monitored 24/7).

*b.* When a breach involves Government-authorized credit cards, the credit card holder must notify the issuing bank immediately upon discovering the breach.

*c.* Report all incidents to the Army Privacy Office (APO) within 24 hours of discovery by entering data into the Privacy Act Tracking System (PATS). PATS populates DD Form 2959 (Breach of Personally Identifiable Information (PII) Report) for processing.

*Note.* It is critical that you retain the number assigned by US-CERT for entry into PATS.

*d.* If computer access is not available, PII compromise can be reported at the 24/7 Army toll free number at 1-866–606–9580.

*e.* The APO processes the actual or suspected breach and sends the appropriate details to DPCLD within 48 hours of discovery. In some cases, the breach report to the Army Privacy Office may occur after the 48-hour time requirement has expired; in these cases, the Army Privacy Office will expedite the processing to DPCLD.

*f.* When the breach includes an actual or suspected compromise of PHI, the Army Privacy Office will also report the incident to the Defense Health Agency Privacy Office within 24 hours of discovery.

*g.* Activities may have additional requirements for reporting compromise incidents. Consult with your privacy officer and follow your activity’s guidance for reporting PII incidents.

*h.* Submit updates to the US-CERT, APO, and the appropriate individual(s) within your activity as additional information becomes available.

### 9–2. Risk assessment and notification determination

*a.* If records containing personal information are lost, stolen, or compromised, the potential exists that the records may be used for unlawful purposes, such as identity theft or fraud. The personal impact on the affected individual(s) may be severe if the records are misused. The activity responsible for safeguarding the PII at the time of the incident may be required to notify the affected individual(s).

*b.* The decision to notify should be made after a risk assessment has been performed to determine the likelihood of harm and the level of risk (potential impact) as a result of the compromise incident. Harm includes embarrassment, inconvenience, financial loss, blackmail, identity theft, emotional stress, and loss of self-esteem. The likely risk of harm and the level of risk will determine when, why, how, and to whom notification should be given.

*c.* Risk assessment is an analysis considering information sensitivity, vulnerabilities, and cost in safeguarding personal information processed or stored at the Army activity.

*d.* The Army activity reporting the breach should weigh the following determination factors to assess the likely risk of harm:

(1) *Nature of the data elements breached.* The nature of the data elements compromised is a key factor to consider in determining when and how notification should be provided to affected individuals. For example, theft of a database containing individuals’ names in conjunction with SSNs, and/or dates of birth may pose a high level of risk of harm, while a theft of a database containing only the names of individuals may pose a lower risk, depending on its context. It is difficult to characterize data elements as creating a low, moderate, or high risk simply based on the type of data because the sensitivity of the data element is contextual. A name in one context may be less sensitive than in another context. For example, breach of a database of names of individuals receiving treatment for contagious disease may pose a higher risk

of harm; whereas, a database of names of subscribers to agency media alerts may pose a lower risk of harm. In assessing the levels of risk and harm, consider the data elements in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals.

(2) *Number of individuals affected.* The magnitude of the number of affected individuals may dictate the method or methods Army activities choose for providing notification, but should not be the determining factor for whether an agency should provide notification.

(3) *Likelihood the information is accessible and usable.* Upon learning of a breach, Activities should assess the likelihood PII will be or has been used by unauthorized individuals. An increased risk that the information will be used by unauthorized individuals should influence the activity's decision to provide notification. The fact the information has been lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals as there may be a number of physical, technological, and/or procedural safeguards in place. If the information is properly protected by encryption, for example, the risk of compromise may be low. Activities should first assess whether the PII is at a low, moderate, or high risk of being compromised. The assessment should be guided by the National Institute of Standards and Technology (NIST) security standards and guidance. Other considerations may include the likelihood any unauthorized individual will know the value of the information and either use the information or sell it to others.

(4) *Likelihood the breach may lead to harm.* The Privacy Act requires agencies to protect against any anticipated threats or hazards to the security or integrity of records which could result in "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." Activities should consider a number of possible harms associated with the loss or compromise of information. Such harms may include the effect the breach has on confidentiality or fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem. The likelihood a breach may result in harm will depend on the manner of the actual or suspected breach and the type(s) of data involved in the incident. Social Security Numbers and account information are useful to committing identity theft, as are name and address or other personally identifying information.

(5) *Ability of the Army activity to mitigate the risk of harm.* Within an information system, the risk of harm will depend on how the agency is able to mitigate further compromise of the system(s) affected by a breach. In addition to containing the breach, appropriate countermeasures, such as monitoring system(s) for misuse of the personal information and patterns of suspicious behavior, should be taken. Such mitigation may not prevent the use of the personal information from identity theft, but it can limit the associated harm. Some harm may be more difficult to mitigate than others, particularly where the potential injury is more individualized and may be difficult to determine.

e. After evaluating each of these factors, activities should reassess the level of impact already assigned to the information using the impact levels defined by NIST. The impact levels of low, moderate, or high describe the (worst case) potential impact on an organization or individual if a breach of security occurs. The levels of potential impact are—

(1) Low if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that the loss of confidentiality, integrity, or availability might cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; resulting in minor damage to organizational assets; minor financial loss; and/or minor harm to individuals.

(2) Moderate if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that the loss of confidentiality, integrity, or availability might cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; resulting in significant damage to organizational assets; significant financial loss; and/or significant harm to individuals that does not involve loss of life or serious life threatening injuries.

(3) High if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that the loss of confidentiality, integrity, or availability might cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; resulting in major damage to organizational assets; major financial loss; and/or severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

f. The impact levels will help determine when and how notification should be provided. Where there is a range of risk levels attributed to the factors, the decision to provide notification should give greater weight to the likelihood the information is accessible and usable and whether the breach may lead to harm. The decision to notify should not be based on one factor alone. A final decision regarding whether to make notification cannot be made until all applicable harm and potential impact have been assessed.

- g. Army activities should carefully evaluate the benefit of notifying the affected individual(s) of low or moderate impact breaches. Leaders should always remain cognizant of the effect that unnecessary notification may have on individuals. Notification when there is little or no risk of harm might create unnecessary concern and confusion.
- h. All breaches rated high impact require notification to the affected individuals.

**9-3. Notification timelines**

The Army activity responsible for safeguarding the PII at the time of the incident must notify the affected individuals after an assessment has been made as to the risk of harm and the level of risk that results from the loss, theft, or compromise of the data. The decision whether to notify an individual rests with the head of the Army activity where the breach occurred. When the actual Army activity where the incident occurred is unknown, by default the responsibility for notifying the affected individuals lies with the originator of the document or information. To reinforce the seriousness of the incident to impacted individuals, notification should be made by an individual at a senior level (for example, commander, director). When notification is necessary, the guidelines are—

- a. Army activities should notify affected individual(s) of a breach assessed as soon as possible, but not later than 10 working days after a breach is discovered and the identity of the individual(s) has been ascertained.
- b. If the Army activity is only able to identify some but not all of the affected individuals, notification should be sent to those who can be identified with follow-up notifications made to those subsequently identified.
- c. If the Army activity cannot readily identify the affected individuals or will not be able to identify the individuals, the activity should provide a generalized notice to the potentially impacted population by whatever means it believes is most likely to reach the affected individuals.
- d. If subject to subparagraph 9-3a, notification of potentially affected individuals has not been made within 10 working days, the Army activity must inform the APO of the reason why notification was not completed and provide a projected completion date.
- e. If breaches involve PII maintained by a contractor, the contractor should take the following steps:
  - (1) Upon discovery and determination that a breach has occurred as a result of a contractor’s actions, the contractor must notify the Army activity or program manager immediately, in accordance with the Army’s established procedures.
  - (2) The Army activity responsible for the breach should determine whether notification is made. If the Army activity determines the contractor is responsible for notifying the impacted individuals, the contractor must submit the notification letters to the activity for review and approval. The activity should coordinate with the contractor to ensure that the notifications requirements as outlined in this section are followed.
- f. The APO will inform DPCLD of the reasons why the notice was not provided to the individuals or the affected population within the 10-day period.
- g. Notification of the affected individuals may be delayed for good cause (for example, law enforcement authorities request delayed notification as immediate notification might jeopardize investigative efforts). When notification is delayed beyond the 10-day period, the APO informs the DPCLD why notice was delayed and provides DPCLD with a projected timeline for notification. The Army provides notification as soon as possible, but consistent with the needs of law enforcement and national security. In these cases, the potential harm to the individual must be weighed against the necessity for delayed notification. Under circumstances where notification could increase risk of harm, the prudent course of action may be to delay notification while appropriate safeguards are put in place.
- h. The notification to the individual, at a minimum, should include—
  - (1) A summary of the events, including the dates of the breach and its discovery.
  - (2) Where names, SSNs, and dates of birth are involved, it is critical that the individual be advised that these data elements potentially have been compromised.
  - (3) The facts and circumstances surrounding the loss, theft, or compromise. The description of the loss should be sufficiently detailed so that the individual clearly understands how the compromise occurred.
  - (4) Preventive actions the Army activity is taking and the individual can take to mitigate against potential future harm. The Army activity should refer the individual to the following Federal Trade Commission (FTC) public Web site when the breach has the potential to result in identity theft for the affected individual: <http://www.consumer.ftc.gov/features/feature-0014-identity-theft>. The FTC site provides valuable information as to what the individuals can do to protect themselves if their identities have been compromised or stolen.
  - (5) A point of contact at the Army activity the individual can reach for additional information, to include the point of contact’s name, phone number, email address, and postal address.

**9-4. Means of providing notification**

The best means for providing notification will depend on the number of individuals affected, available contact information, and the urgency with which the affected individual needs to receive notice.

*a.* First-class mail notification should be the primary means by which notification is provided. Written notification should be sent to the affected individual's last known mailing address in your activity's records. Where you have reason to believe the address is no longer current, you should take reasonable steps to obtain updated mailing information by consulting with other agencies such as the U.S. Postal Service. The front of the envelope should be labeled to alert the recipient to the importance of its contents, for example, "Data Breach Information Enclosed."

*b.* Telephone notification may be appropriate in cases where urgency may dictate immediate and personalized notification and/or when a limited number of individuals are affected. A written notification by first-class mail should immediately follow the telephone notification.

*c.* E-mail notification may also be employed in conjunction with postal mail if the circumstances of the breach warrant this approach. Notification by e-mail may be appropriate where an individual has provided an e-mail address, has expressly given consent to e-mail as the primary means of communication, and no known mailing address is available. However, e-mail notifications may be problematic because individuals change their e-mail addresses and often do not notify third parties of the change.

*d.* Newspapers or other public media outlets may be appropriate in cases where the breach is significant (for example, impacting thousands of individuals, the PII 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. The actions taken to inform the media are necessary to preserve the public's trust. Activities should also set up toll-free call centers staffed by trained personnel to handle inquiries from the affected individuals and the public.

*e.* A generalized substitute notice should be given to the potentially impacted population by whatever means the activity believes is most likely to reach the impacted individuals.

#### **9–5. Risk mitigation**

*a.* For all breaches, but especially for high impact breaches, the Army activity should assemble an After Action Review team to assess the severity of each incident, especially high impact risk, and extract lessons learned to prevent future breaches (per NIST Special Publication 800–122).

*b.* During the process of collecting and analyzing lessons learned, preventive steps can be taken to mitigate the results of identity theft, to minimize the risk of future breaches, and to expand the knowledge base of lessons learned for training development and delivery purposes.

*c.* Information learned through detection, analysis, containment, and recovery should be collected for sharing within the organization to help protect against further incidents.

*d.* Army activities should determine whether administrative or disciplinary action is warranted and appropriate for those individuals determined to be responsible for the loss, theft, or compromise

*e.* When a breach involves personal credit cards, Army activities have the discretion to offer some assistance, such as credit monitoring. However, individuals can self-monitor and can obtain free credit reports from the credit monitoring agencies, as well as have a fraud alert posted on their credit file. Posting a fraud alert usually involves no direct cost to the Government or to the individual; however, inconvenience and indirect costs may be unavoidable. The FTC provides credit guidance on its Web site at: <http://www.ftc.gov/bcp/edu/microsites/idtheft/>.

*f.* The FTC urges credit cardholders to immediately place a fraud alert after a credit card is lost or stolen. The fraud alert is for a period of 90 days, during which creditors assist the cardholder with preventive and protective actions. The FTC site provides valuable information that can be taken immediately or in the future if problems should develop.

*g.* GSA awarded blanket purchase agreements (BPAs) to assist Federal agencies in protecting the confidentiality of personal and credit and payment information, as well as providing a fast and effective solution for Federal agencies needing commercial-off-the-shelf credit monitoring. These agreements allow Federal agencies to take advantage of significantly reduced unit pricing and volume discounting. GSA provides BPA guidance on its Web site at <http://www.gsa.gov/portal/content/199353>.

*h.* Army activities can choose different levels of credit monitoring services depending on the degree of vulnerability, risk, and protection. The BPAs also eliminate separate contracting and open market costs that result from separate agencies searching for sources, developing technical documents and solicitations, and evaluating offers.

#### **9–6. Completion of Privacy Act Tracking System submission**

A PATS entry must be submitted according to the abovementioned timelines and must include the following reportable information (see paragraph 9–1):

- a.* Date of breach, date discovered, and date reported to US-CERT.
- b.* US-CERT number and Component Internal Tracking Number (if applicable).
- c.* Component and office name.

- d. Point of contact information including name, duty phone, and office mailing address.
- e. Narrative description of breach including—
  - (1) The parties involved in the breach.
  - (2) The media used such as email, info-sharing, paper records, or equipment.
  - (3) Type of breach: loss, theft, or compromise.
  - (4) Immediate steps taken to contain the breach.
- f. Mitigating actions taken including—
  - (1) Whether the breach was intentional or inadvertent.
  - (2) Any lessons learned.
- g. Number of individuals affected (including numbers of Soldiers, civilians, and contractors involved).
- h. Type of PII compromised such as SSN, PHI, and financial information.
- i. Any additional information as indicated on DD Form 2959.
- j. Once DD Form 2959 is completed, the breach reporting individual should submit it as indicated above.
- k. If computer access is not available, PII incidents can be reported at the 24/7 toll free number of 1-866-606-9580.

### **9-7. Additional breach reporting resources**

- a. Additional information about breach reporting and sample items such as the PII incident reporting template and a sample notification letter are available at Web site: <http://www.rmda.army.mil/privacy/rmda-po-division.html>.
- b. PHI, a subset of PII, is defined by the Health Insurance Portability and Accountability Act of 1996 and in DOD 6025.18-R. Additional guidance on breach reporting involving PHI is available at Web site: <http://www.hhs.gov/ocr/privacy/>.

## **Chapter 10 Privacy Act Complaints and Judicial Sanctions**

### **10-1. Privacy Act complaints**

- a. The installation-level privacy official is responsible for processing Privacy Act complaints or allegations of Privacy Act violations. Guidance should be sought from the local Staff Judge Advocate and coordination made with the system manager to assist in the resolution of Privacy Act complaints. The local privacy official is responsible for reviewing allegations of Privacy Act violations and the evidence provided by the complainants. The local privacy official also makes an initial assessment as to the validity of the complaint, and takes appropriate corrective or mitigating action.
- b. The local privacy official coordinates with the local Staff Judge Advocate to determine whether a more substantive investigation such as a commander's inquiry or an AR 15-6 investigation is appropriate. The local privacy official also ensures that the complaint resolution or the decision from a more formal investigation is provided to the complainant in writing. The decision at the local level may be appealed to the next higher command level privacy official. A legal review from the next higher command level privacy official's servicing Staff Judge Advocate is required prior to action on the appeal.

### **10-2. Judicial sanctions**

The Privacy Act has both civil remedies and criminal penalties for violations of its provisions.

- a. *Civil remedies.* An individual may file a civil suit against DA if Army personnel fail to comply with the Privacy Act. In addition to specific remedial actions, 5 USC 552a(g) may provide for the payment of damages, court costs, and attorney's fees.
- b. *Criminal penalties.* A member or employee of the Army may be found guilty of a misdemeanor and fined not more than \$5,000 for—
  - (1) Willfully maintaining a system of records without first meeting the public notice requirements of publishing in the Federal Register;
  - (2) Willfully disclosing information from a system of records, knowing that the disclosure is prohibited to one not entitled to receive it; or
  - (3) Knowingly and willfully requesting or obtaining any record concerning an individual from an agency under false pretenses.

## Chapter 11 Training Requirements and Resources

### 11–1. Training requirements

The Privacy Act requires all heads of Army activities, Army Staff agencies, field operating agencies, direct reporting units, subordinate commands, and installations to establish rules of conduct for all personnel involved in the design, development, operation, and maintenance of any Privacy Act system of records and to train the appropriate personnel with respect to the privacy rules including the penalties for noncompliance. To meet these training requirements, Army commanders and system managers are required to implement and maintain annual duty-specific Privacy Act training. All Army personnel, including contractors, must complete annual refresher Privacy training. Local privacy officers must maintain records of completion by any method (for example, by spreadsheet). Five general levels of training should be established and various training tools should be implemented:

*a. Orientation.* The initial training, given to all personnel, provides a basic understanding of the Privacy Act and this regulation as it applies to the individual's job performance. This training will be provided to Army personnel and contractors who maintain PII, and should be a prerequisite to all other levels of training. Army personnel who mishandle PII are required to take refresher training.

*b. Specialized.* Training that addresses the application of specific provisions of this regulation to specialized areas of job performance. Personnel of particular concern include personnel specialists, finance officers, Army personnel who deal with the news media or the public, special investigators, paperwork managers, individuals working with medical and security records, records managers, computer systems development personnel, computer systems operations personnel, statisticians dealing with personal data and program evaluations, contractors, and anyone responsible for implementing or carrying out functions under this regulation. Specialized training should be provided on a periodic basis. Remedial and refresher training should be customized for the specialized areas.

*c. Managerial.* Training designed to identify and clarify for responsible managers (such as senior system managers, denial authorities, and functional managers) issues that they should consider when making management decisions affected by the Army Privacy Program.

*d. Annual Privacy Act Refresher Training.* Annual refresher training, in accordance with assigned responsibilities, will be provided to ensure Army personnel and contractors continue to understand their specific responsibilities for information protected by the Privacy Act.

*e. Additional or Advanced Training.* Additional or advanced training should be provided to Army personnel and contractors after a change in official duties resulting in increased responsibilities. Ideally this training is duty-specific; for operational reasons, mandatory IA training may be adequate for meeting this requirement.

### 11–2. Training records

*a.* Army privacy officers are to maintain a record of training completion status. Training records will be retained in either a central electronic personnel record or local office training system. For Army contractors, the training record of completion will be retained by the appropriate office supported by the contract. Each trainee should retain a copy of privacy training completion documentation for their records.

*b.* The training record, demonstrating Privacy Act training completion, may be subject to inspection during reviews by Army privacy officials, the Inspector General of the Department of Defense, or Army's Inspector General. Additionally, each Army privacy officer should be able to demonstrate training completion rates for each category of personnel.

*c.* Each Army activity should examine their training, and, if necessary, expand their training materials and program to include specific privacy and security awareness segments.

### 11–3. Training materials

The Army Privacy Office provides training materials on the RMDA Web site: <https://www.rmda.army.mil/index.html>. The materials include an online Privacy Act Overview course, PII breach management and information assurance (IA) documents, access to external related educational opportunities, and a link to the DPCLD Web site: <http://dpclد.defense.gov/privacy>, which includes an assortment of privacy-related resources and publications.

### 11–4. Conceptual training

One of the goals of Privacy Act training is to ensure that the Army culture in each Army organization has been infused with the spirit of privacy in addition to the routine requirements. The framework for this cultural awareness training includes the following concepts:

- a.* Managers ensure that all personnel are informed of requirements to protect the privacy of individuals and their records.
- b.* Army personnel safeguard PII in order to preserve security and confidentiality, and to avoid illegal disclosure of PII; and report any unauthorized disclosures.
- c.* Army leaders must be aware of record handling procedures, ensure that personnel receive adequate training, keep system notices current and correct, and diligently observe all FR and DOD Privacy Program requirements.
- d.* According to the Defense Information Systems Agency, the majority of privacy breaches and security problems occur from internal users rather than external users. Moreover, the breaches are usually the result of careless human error rather than malicious behavior. The safeguarding of PII is directly and indirectly related to national security.
- e.* IA training, which is required annually, emphasizes the strong overlapping interface between privacy and security.

## **Appendix A**

### **References**

#### **Section I**

##### **Required Publications**

Unless otherwise stated, all publications are available at <http://www.apd.army.mil/>. Department of Defense regulations are available at <http://www.dtic.mil/>. Public Laws, United States Codes, and Code of Federal Regulations are available at <http://www.gpo.gov/fdsys/search/home.action>.

##### **AR 15–6**

Procedures for Investigating Officers and Boards of Officers (Cited in para 10–1*b*.)

##### **AR 25–1**

Army Information Technology (Cited in para 1–9*a*(4).)

##### **AR 25–2**

Information Assurance (Cited in para 1–8*b*(3).)

##### **AR 25–400–2**

The Army Records Information Management System (ARIMS) (Cited in para 1–6.)

##### **AR 195–2**

Criminal Investigation Activities (Cited in para 8–1*f*.)

##### **PL 108–458**

Intelligence Reform and Terrorism Protection Act of 2004 (Cited in para 3–3*p*.)

##### **PL 110–53**

Implementing Recommendations of the 9/11 Commission Act of 2007 (Cited in para 2–4*c*(7).)

#### **Section II**

##### **Related Publications**

A related publication is a source of additional information. The user does not have to read the publication to understand this regulation. The Federal Acquisition Regulation is available at <http://www.acquisition.gov/far/>. Executive orders are available at <http://www.archives.gov/federal-register/executive-orders/disposition.html/>. Public Laws, United States Codes, and Code of Federal Regulations are available at: <http://www.gpo.gov/fdsys/search/home.action>.

##### **AR 10–87**

Army Commands, Army Service Component Commands, and Direct Reporting Units

##### **AR 11–2**

Managers' Internal Control Program

##### **AR 20–1**

Inspector General Activities and Procedures

##### **AR 25–30**

The Army Publishing Program

##### **AR 25–55**

Department of the Army Freedom of Information Act Program

##### **AR 27–10**

Military Justice

##### **AR 27–40**

Litigation

##### **AR 36–2**

Audit Services in the Department of the Army

##### **AR 40–66**

Medical Record Administration and Health Care Documentation

**AR 190–45**

Law Enforcement Reporting

**AR 215–8/AFI 34–211(I)**

Army and Air Force Exchange Service Operations

**AR 380–5**

Department of Army Information Security Program

**AR 600–37**

Unfavorable Information

**AR 630–10**

Absence without Leave, Desertion, and Administration of Personnel Involved in Civilian Court Proceedings

**AR 633–30**

Military Sentences to Confinement

**DA Pam 25–403**

Guide to Recordkeeping in the Army

**DOD 5200.1–R**

DOD Information Security Program Regulation, January 1997

**DOD 5400.7–R**

DOD Freedom of Information Act Program

**DOD 5400.11–R**

DOD Privacy Program

**DOD 6025.18–R**

DOD Health Information Privacy Regulation

**DOD 7750.07–M**

DOD Forms Management Program Procedures Manual

**DOD 8910.01–M**

DOD Information Collections Manual: Procedures for DOD Internal Information Collections

**DODD 5105.53**

DOD Director of Administration and Management (DA&M)

**DODD 5400.7**

DOD Freedom of Information Act Program

**DODD 5400.11**

DOD Privacy Program

**DODD 8500.01E**

Information Assurance (IA)

**DODI 1000.29**

DOD Civil Liberties Program

**DODI 1000.30**

Reduction of Social Security Number (SSN) Use within DOD

**DODI 1332.28**

Discharge Review Board (DRB) Procedures and Standards

**DODI 5400.04**

Provision of Information to Congress

**DODI 5400.16**

DOD Privacy Impact Assessment (PIA) Guidance

**DODI 7650.01**

General Accounting Office Access and Comptroller General Requests for Access to Records

**DODI 8550.01**

DOD Internet Services and Internet-Based Capabilities

**DODI 8910.01**

Information Collection and Reporting

**EO 9397**

Numbering System for Federal Accounts Relating to Individual Persons

**EO 11862**

Amending Executive Order No. 11652 Relating to Classification and Declassification of National Security Information and Material

**EO 12333**

United States Intelligence Activities

**EO 12356**

National Security Information

**EO 13388**

Further Strengthening the Sharing of Terrorism Information to Protect Americans

**EO 13402**

Strengthening Federal Efforts to Protect Against Identity Theft

**Federal Register, Volume 40**

Office of Management and Budget, Privacy Act Implementation (Available at <https://www.federalregister.gov/>.)

**Federal Register, Volume 54**

Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988

**FIPS Publication 199**

Standards for Security Categorization of Federal Information and Information Systems (Available at <http://csrc.nist.gov/>.)

**NIST Special Publication 800-122**

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (Available at <http://csrc.nist.gov/>.)

**OMB Circular A-19**

Legislative Coordination and Clearance (Available at <http://www.whitehouse.gov/>.)

**OMB Circular A-130**

Transmittal Memorandum No. 4: Management of Federal Information Resources (Available at <http://www.whitehouse.gov/>.)

**OMB Memorandum M-05-08**

Designation of Senior Agency Officials for Privacy (Available at <http://www.whitehouse.gov/>.)

**OMB Memorandum M-07-16**

Safeguarding Against and Responding to the Breach of Personally Identifiable Information (Available at <http://www.whitehouse.gov/>.)

**OMB Memorandum 10-23**

Guidance for Agency Use of Third-Party Websites and Applications (Available at <http://www.whitehouse.gov/>.)

**PL 100-503**

Computer Matching and Privacy Protection Act of 1988

**PL 105-318, Section 3007**

The Identity Theft and Assumption Deterrence Act of 1998

**PL 107-347, Section 208**

Privacy Provisions, Electronic Government (E-Gov) Act of 2002

**PL 108-458, As Amended Through PL 113-293**

Intelligence Reform and Terrorism Prevention Act of 2004

**Treasury Fiscal Requirements Manual, Bulletin No. 76-07**

Department of the Treasury Fiscal Requirements Manual (Available at <http://tfm.fiscal.treasury.gov/>)

**5 CFR 293, 294, 297, and 7351**

Army Privacy Act Program

**5 CFR 310**

DOD Privacy Program

**5 CFR 505**

Army Privacy Act Program

**48 CFR 24**

Protection of Privacy and Freedom of Information

**5 USC 552**

Freedom of Information Act (FOIA)

**5 USC 552a**

Records maintained on individuals

**5 USC 1205**

Transmittal of information to Congress

**5 USC 1206**

Annual report

**5 USC 5516**

Withholding District of Columbia income taxes

**5 USC 5517**

Withholding State income taxes

**5 USC 5520**

Withholding of city or county income or employment taxes

**6 USC 482**

Facilitating Homeland Security Information Sharing Procedures

**6 USC 485**

Information sharing

**10 USC 130b**

Personnel in overseas, sensitive, or routinely deployable units: nondisclosure of personally identifiable information

**10 USC 1553**

Review of Discharge or Dismissal

**10 USC 3013**

Records maintained on individuals

**13 USC 8**

Authenticated Transcripts or Copies of Certain Returns; Other Data; Restriction on Use; Disposition of Fees Received

**18 USC 3056**

Powers, Authorities, and Duties of United States Secret Service

**28 USC 1746**

Unsworn Declarations Under Penalty of Perjury

**28 USC 15704**

Inspector General; Records

**44 USC Chapter 33**

Disposal of Records

**44 USC 3102**

Establishment of Program of Management

### **Section III**

#### **Prescribed Forms**

This section contains no entries.

### **Section IV**

#### **Referenced Forms**

Unless otherwise indicated, DA forms are available on the APD Web site (<http://www.apd.army.mil>); DD forms are available on DOD Web site (<http://www.dtic.mil/>).

#### **DA Form 11-2**

Internal Control Evaluation Certification

#### **DA Form 2028**

Recommended Changes to Publications and Blank Forms

#### **DD Form 2923**

Privacy Act Data Cover Sheet

#### **DD Form 2930**

Privacy Impact Assessments

#### **DD Form 2959**

Breach of Personally Identifiable Information (PII) Report

#### **IRS Form W-2**

Wage and Tax Statement (Available at <https://www.srs.gov/forms-pubs>)

#### **SF 50**

Notification of Personnel Action (Available at <http://www.gsa.gov/>)

## **Appendix B**

### **Denial Authorities**

#### **B-1. The Administrative Assistant to the Secretary of the Army**

The AASA acts for the Secretary of the Army on requests for all records maintained by the Office of the Secretary of the Army and its serviced activities, as well as requests requiring the personal attention of the Secretary of the Army. This includes civilian Equal Employment Opportunity (EEO) actions. The Administrative Assistant to the Secretary of the Army has delegated this authority to the Chief Attorney, OAASA. See Deputy Chief of Staff, G-1 for Military Equal Opportunity actions.

#### **B-2. The Assistant Secretary of the Army (Financial Management and Comptroller)**

The ASA(FM&C) acts on requests for finance and accounting records. Requests for continental United States (CONUS) finance and accounting records should be referred to the Defense Finance and Accounting Service. The Chief Attorney, OAASA, acts on requests for non-finance and accounting records of the Assistant Secretary of the Army (Financial Management and Comptroller).

#### **B-3. The Deputy Assistant Secretary of the Army (Manpower and Reserve Affairs)**

The DASA(M&RA) acts on requests for civilian personnel records, personnel administration, and other civilian personnel matters, except for EEO (civilian) matters which will be acted on by the Administrative Assistant to the Secretary of the Army. Requests from former civilian employees to amend a record in an Office of Personnel Management system of records, such as the Official Personnel Folder, should be sent to the Office of Personnel Management: 1900 E. Street, NW, Washington, DC 20415-1000.

#### **B-4. The Inspector General**

TIG acts on requests for all records held by The Inspector General. Resolutions will either be coordinated by Office of The Inspector General for HQDA actions or by the U.S. Army Inspector General Agency for field actions.

#### **B-5. The Army Auditor General**

TAG acts on requests for records relating to audits done by the U.S. Army Audit Agency under AR 10-2. This includes requests for related records developed by the Audit Agency.

#### **B-6. The Director of the Army Staff**

The DAS acts on requests for all records of the Chief of Staff and its Field Operating Agencies. The Director of the Army Staff has delegated this authority to the Chief Attorney and Legal Services, Office of the Administrative Assistant to the Secretary of the Army (see The Judge Advocate General for the General Officer Management Office actions).

#### **B-7. The Deputy Chief of Staff, G-1**

The DCS, G-1 acts on the following records: Personnel board records, Equal Opportunity (military) and sexual harassment, health promotions, physical fitness and well-being, except for individual treatment records which are the responsibility of the Surgeon General, retiree benefits, services, and programs.

#### **B-8. The Deputy Chief of Staff, G-2**

The DCS, G-2 acts on requests for records relating to intelligence and counterintelligence activities.

#### **B-9. The Surgeon General**

TSG acts on requests for medical records of active duty military personnel, dependents, and persons given physical examination or treatment at DA medical facilities, to include alcohol and drug treatment and/or test records.

#### **B-10. The Chief of Chaplains**

The CCH acts on requests for records involving ecclesiastical relationships, rites performed by DA chaplains, and nonprivileged communications relating to clergy and active duty chaplains' military personnel files.

#### **B-11. The Judge Advocate General**

TJAG acts on requests for records relating to claims, courts-martial, legal services, administrative investigations, and similar legal records. In addition, the Office of the Judge Advocate General (OTJAG) is authorized to act on requests for

records that are not within the functional areas of responsibility of any other denial authority, including, but not limited to requests for records for commands and activities.

#### **B-12. The Chief, National Guard Bureau**

The CNGB acts on requests for all personnel and medical records of retired, separated, discharged, deceased, and Active Army National Guard military personnel, including technician personnel, unless such records clearly fall within another denial authority's responsibility. This authority includes, but is not limited to, National Guard organization and training files; plans, Equal Opportunity investigative records; aviation program records and financial records dealing with personnel, operation and maintenance, and equipment budgets.

#### **B-13. The Chief, Army Reserve**

The CAR acts on requests for all personnel and medical records of retired, separated, discharged, deceased, and Reserve Component military personnel, and all U.S. Army Reserve (USAR) records, unless such records clearly fall within another denial authority's responsibility. Records under the responsibility of the Chief, Army Reserve include records relating to USAR plans, policies, and operations; changes in the organizational status of USAR units; and all other Office of the Chief, Army Reserve records and Headquarters, U.S. Army Reserve Command records.

#### **B-14. The Provost Marshal General**

The PMG acts on all requests for provost marshal activities and law enforcement functions for the Army.

#### **B-15. The Commander, U.S. Army Criminal Investigation Command**

The Commander, USACIDC, acts on requests for criminal investigative records of USACIDC headquarters, and its subordinate activities, and military police reports. This includes criminal investigation records, investigation-in-progress records, and all military police records and reports that result in criminal investigation reports. This authority has been delegated to the Director, U.S. Army Crime Records Center.

#### **B-16. The Commander, U.S. Army Human Resources Command**

The Commander, USAHRC, acts on requests for military personnel files relating to active duty personnel including, but not limited to military personnel matters, military education records including records related to the removal or suspension from a military school or class; personnel locator, physical disability determinations, and other military personnel administration records; records relating to military casualty and memorialization activities; heraldic activities, voting, records relating to identification cards, naturalization and citizenship, commercial solicitation, Military Postal Service Agency and Army postal and unofficial mail service. The Commander, U.S. Army Human Resources Command, is also authorized to act on requests concerning all personnel and medical records of retired, separated, discharged, deceased, and Reserve Component military personnel, unless such records clearly fall within another denial authority's functional area. This authority includes all personnel and medical records of retired, separated, discharged, deceased, and Reserve Component military personnel, unless such records clearly fall within another denial authority's functional area.

#### **B-17. The Commander, U.S. Army Combat Readiness Center**

The Commander, USACRC, acts on requests for Army safety records.

#### **B-18. The General Counsel, Army and Air Force Exchange Service**

The GC, AAFES, acts on requests for Army and Air Force Exchange Service records, under AR 215-8/Air Force Instruction (AFI) 34-211(I).

#### **B-19. The Commander, Military Surface Deployment and Distribution Command**

The Commander, MSDDC acts on requests for records pertaining to military and commercial transportation and traffic management records.

#### **B-20. Special Denial Authority**

Special denial authority delegates for time-event related records may be designated on a case-by-case basis. Special denial authority delegations will be published in the Federal Register. To obtain current information on special delegations, contact the Department of the Army, Freedom of Information and Privacy Office.

## Appendix C

### Exempt Army and Office of Personnel Management Records

#### C-1. Exempt Army records

The following records may be exempt from certain parts of the Privacy Act:

*a.* System identifier: A0020-1 SAIG.

(1) System name: Inspector General Records.

(2) Exemptions: Portions of this system of records may be exempt pursuant to 5 USC 552a(k)(2) and (k)(5) from subsections 5 USC 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f).

(3) Authority: 5 USC 552a(k)(2) and (k)(5).

(4) Reasons:

*(a)* From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

*(b)* From subsection (d) because access to such records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

*(c)* From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violations of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information is retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

*(d)* From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from the access provisions of subsection (d), making these subsections not applicable.

*(e)* From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

*(f)* From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

*b.* System identifier: A0 025-400-2 OAA.

(1) System name: Army Records Information Management System (ARIMS).

(2) Exemption: During the course of records management, declassification, and claims research, exempt materials from other systems of records may in turn become part of the case record in this system. To the extent that copies of exempt records from those "other" systems of records are entered into this system, the Department of the Army hereby claims the same exemptions for the records from those "other" systems.

(3) Authority: 5 USC 552a (j)(2) and (k)(1) through (k)(7).

(4) Reasons: Records are only exempt from pertinent provisions of 5 USC 552a to the extent such provisions have been identified and an exemption claimed for the original record and the purposes underlying the exemption for the original record still pertain to the record which is now contained in this system of records. In general, the exemptions were claimed in order to protect properly classified information relating to national defense and foreign policy, to avoid interference during the conduct of criminal, civil, or administrative actions or investigations, to ensure protective services provided to the President and others are not compromised, to protect records used solely as statistical records, to protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations, to preserve the confidentiality and integrity of Federal testing materials, and to safeguard evaluation materials used for military promotions when furnished by a confidential source. The exemption rule for the original records will identify the specific reasons why the records may be exempt from specific provisions of 5 USC 552a.

*c.* System identifier: A0025-2 PMG (DFBA) DOD.

(1) System name: Defense Biometrics Identification Records System.

(2) Exemptions: Portions of this system of records may be exempt pursuant to 5 USC 552a(j)(2) and (k)(2) from subsections 5 USC 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g).

(3) Authority: 5 USC 552a(j)(2) and (k)(2).

(4) Reasons:

*(a)* From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (c)(4) because an exemption is being claimed for subsection (d), making this subsection not applicable.

(c) From subsection (d) because access to such records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(d) From subsection (e)(1) because the nature of the criminal and/or civil investigative function creates unique problems in prescribing a specific parameter in a particular case with respect to what information is relevant or necessary. Also, information may be received which may relate to a case under the investigative jurisdiction of another agency. The maintenance of this information may be necessary to provide leads for appropriate law enforcement purposes and to establish patterns of activity that may relate to the jurisdiction of other cooperating agencies.

(e) From subsection (e)(2) because in a criminal investigation, the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection.

(f) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life and physical safety of confidential informants.

(g) From subsections (e)(4)(G) and (e)(4)(H) because the requirements in those subsections are inapplicable to the extent that portions of this system of records may be exempt from subsection (d), concerning individual access.

(h) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(i) From subsection (e)(5) because in the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of intelligence necessary for effective law enforcement.

(j) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue search authorizations and could reveal investigative techniques and procedures.

(k) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

(l) From subsection (g) because portions of this system of records are compiled for law enforcement purposes and have been exempted from the access provisions of subsections (d) and (f).

d. System identifier: A0025-55 OAA.

(1) System name: Freedom of Information Act Program Files.

(2) Exemption: During the processing of Freedom of Information Act (FOIA) requests, exempt materials from other systems of records may in turn become part of the case record in this system. To the extent that copies of exempt records from those "other" systems of records are entered into this system, the Department of the Army claims the same exemptions for the records from those "other" systems.

(3) Authority: 5 USC 552a(j)(2) and (k)(1) through (k)(7).

(4) Reasons: Records are only exempt from pertinent provisions of 5 USC 552a to the extent such provisions have been identified and an exemption claimed for the original record and the purposes underlying the exemption for the original record still pertain to the record which is now contained in this system of records. In general, the exemptions were claimed in order to protect properly classified information relating to national defense and foreign policy, to avoid interference during the conduct of criminal, civil, or administrative actions or investigations, to ensure protective services provided to the President and others are not compromised, to protect records used solely as statistical records, to protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations, to preserve the confidentiality and integrity of Federal testing materials, and to safeguard evaluation materials used for military promotions when furnished by a confidential source. The exemption rule for the original records will identify the specific reasons why the records may be exempt from specific provisions of 5 USC 552a.

e. System identifier: A0027-1 DAJA.

(1) System name: General Legal Files.

(2) Exemption: Portions of this system of records may be exempt pursuant to 5 USC 552a(k)(1) through(k)(7) from subsections 5 USC 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f).

(3) Authority: 5 USC 552a(k)(1), (k)(2), (k)(5), (k)(6), and (k)(7).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (d) because access to such records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(c) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violations of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information is retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(d) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from the access provisions of subsection (d), making these subsections not applicable.

(e) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(f) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

f. System identifier: A0027-10a DAJA.

(1) System name: Military Justice Files.

(2) Exemptions: Portions of this system of records may be exempt pursuant to 5 USC 552a(j)(2) from subsections 5 USC 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g).

(3) Authority: 5 USC 552a(j)(2).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (c)(4) because an exemption is being claimed for subsection (d), making this subsection not applicable.

(c) From subsection (d) because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(d) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(e) From subsection (e)(2) because in a criminal investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection.

(f) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life and physical safety of confidential informants.

(g) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from the access provisions of subsection (d), making these subsections not applicable.

(h) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(i) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would

restrict the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of intelligence necessary for effective law enforcement.

(j) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue search authorizations and could reveal investigative techniques and procedures.

(k) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

(l) From subsection (g) because portions of this system of records are compiled for law enforcement purposes and have been exempted from the access provisions of subsections (d) and (f).

g. System identifier: A0027-10b DAJA.

(1) System name: Courts-Martial Records and Reviews.

(2) Exemptions: Portions of this system of records may be exempt pursuant to 5 USC 552a(j)(2) from subsections 5 USC 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g).

(3) Authority: 5 USC 552a(j)(2).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (c)(4) because an exemption is being claimed for subsection (d), making this subsection not applicable.

(c) From subsection (d) because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(d) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(e) From subsection (e)(2) because in a criminal investigation, the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection.

(f) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life and physical safety of confidential informants.

(g) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from the access provisions of subsection (d), making these subsections not applicable.

(h) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(i) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of intelligence necessary for effective law enforcement.

(j) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue search authorizations and could reveal investigative techniques and procedures.

(k) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

(l) From subsection (g) because portions of this system of records are compiled for law enforcement purposes and have been exempted from the access provisions of subsections (d) and (f).

h. System identifier: A0040-5b DASG.

(1) System name: Army Public Health Data Repository (APHDR).

(2) Exemption: Portions of this system of records may be exempt pursuant to 5 USC 552a(k)(2) and (k)(4) from subsections 5 USC 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f).

(3) Authority: 5 USC 552a(k)(2) and (k)(4).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (d) because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(c) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violations of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information is retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(d) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from the access provisions of subsection (d), making these subsections not applicable.

(e) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(f) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

*i.* System identifier: A0190-5 OPMG.

(1) System name: Vehicle Registration System.

(2) Exemption: Portions of this system of records may be exempt pursuant to 5 USC 552a(j)(2) from subsections 5 USC 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(8), (f), and (g).

(3) Authority: 5 USC 552a(j)(2).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (c)(4) because an exemption is being claimed for subsection (d), making this subsection not applicable.

(c) From subsection (d) because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(d) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(e) From subsection (e)(2) because in a criminal investigation, the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection.

(f) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life and physical safety of confidential informants.

(g) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from access provisions of subsection (d), making these subsections not applicable.

(h) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(i) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would

restrict the ability of trained investigators and intelligence analysts to exercise their judgment reporting on investigations and impede the development of intelligence necessary for effective law enforcement.

(j) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue search authorizations and could reveal investigative techniques and procedures.

(k) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

(l) From subsection (g) because portions of this system of records are compiled for law enforcement purposes and have been exempted from the access provisions of subsections (d) and (f).

j. System identifier: A0190-9 OPMG.

(1) System name: Absentee Case Files.

(2) Exemption: Portions of this system of records may be exempt pursuant to 5 USC 552a(j)(2) from subsections 5 USC 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(8), (f), and (g).

(3) Authority: 5 USC 552a(j)(2).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (c)(4) because an exemption is being claimed for subsection (d), making this subsection not applicable.

(c) From subsection (d) because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(d) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(e) From subsection (e)(2) because in a criminal investigation, the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection.

(f) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life and physical safety of confidential informants.

(g) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from access provisions of subsection (d), making these subsections not applicable.

(h) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(i) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment reporting on investigations and impede the development of intelligence necessary for effective law enforcement.

(j) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue search authorizations and could reveal investigative techniques and procedures.

(k) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

(l) From subsection (g) because portions of this system of records are compiled for law enforcement purposes and have been exempted from the access provisions of subsections (d) and (f).

k. System identifier: A0190-14 OPMG.

(1) System name: Registration and Permit Files.

(2) Exemption: Portions of this system of records may be exempt pursuant to 5 USC 552a(k)(2) from subsections 5 USC 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f).

(3) Authority: 5 USC 552a(k)(2).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (d) because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(c) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violations of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information is retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(d) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from the access provisions of subsection (d), making these subsections not applicable.

(e) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(f) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

l. System identifier: A0190-45 OPMG.

(1) System name: Military Police Reporting Program Records (MPRP).

(2) Exemptions: Portions of the system may be exempt pursuant to 5 USC 552a(j)(2) from subsections 5 USC 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g).

(3) Authority: 5 USC 552a(j)(2).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (c)(4) because an exemption is being claimed for subsection (d), making this subsection not applicable.

(c) From subsection (d) because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(d) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(e) From subsection (e)(2) because in a criminal investigation, the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection.

(f) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life and physical safety of confidential informants.

(g) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from access provisions of subsection (d), making these subsections not applicable.

(h) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(i) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would

restrict the ability of trained investigators and intelligence analysts to exercise their judgment reporting on investigations and impede the development of intelligence necessary for effective law enforcement.

(j) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue search authorizations and could reveal investigative techniques and procedures.

(k) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

(l) From subsection (g) because portions of this system of records are compiled for law enforcement purposes and have been exempted from the access provisions of subsections (d) and (f).

m. System identifier: A0190-45a OPMG.

(1) System name: Local Criminal Intelligence Files.

(2) Exemptions: Portions of the system of records may be exempt pursuant to 5 USC 552a(j)(2) from subsections 5 USC. 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(8), (f), and (g).

(3) Authority: 5 USC 552a(j)(2).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (c)(4) because an exemption is being claimed for subsection (d), making this subsection not applicable.

(c) From subsection (d) because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(d) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(e) From subsection (e)(2) because in a criminal investigation, the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection.

(f) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life and physical safety of confidential informants.

(g) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from access provisions of subsection (d), making these subsections not applicable.

(h) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(i) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment reporting on investigations and impede the development of intelligence necessary for effective law enforcement.

(j) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue search authorizations and could reveal investigative techniques and procedures.

(k) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

(l) From subsection (g) because portions of this system of records are compiled for law enforcement purposes and have been exempted from the access provisions of subsections (d) and (f).

n. System identifier: A0190-45b OPMG.

(1) System Name: Serious Incident Reporting Files.

(2) Exemptions: Portions of the system of records may be exempt pursuant to 5 USC 552a(j)(2) from subsections 5 USC 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(8), (f), and (g).

(3) Authority: 5 USC 552a(j)(2).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (c)(4) because an exemption is being claimed for subsection (d), making this subsection not applicable.

(c) From subsection (d) because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(d) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(e) From subsection (e)(2) because in a criminal investigation, the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection.

(f) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life and physical safety of confidential informants.

(g) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from access provisions of subsection (d), making these subsections not applicable.

(h) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(i) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment reporting on investigations and impede the development of intelligence necessary for effective law enforcement.

(j) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue search authorizations and could reveal investigative techniques and procedures.

(k) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

(l) From subsection (g) because portions of this system of records are compiled for law enforcement purposes and have been exempted from the access provisions of subsections (d) and (f).

*o.* System identifier: A0190-47 DAPM-ACC.

(1) System Name: Army Corrections System and Parole Board Records.

(2) Exemptions: Portions of the system of records may be exempt pursuant to 5 USC 552a(j)(2) from subsections 5 USC 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g).

(3) Authority: 5 USC 552a(j)(2).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (c)(4) because an exemption is being claimed for subsection (d), making this subsection not applicable.

(c) From subsection (d) because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(d) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(e) From subsection (e)(2) because in a criminal or other law enforcement investigation, the requirement that information be collected to the greatest extent possible from the subject individual would alert the subject as to the nature or existence of the investigation and thereby present a serious impediment to effective law enforcement.

(f) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life and physical safety of confidential informants.

(g) From subsections (e)(4)(G) and (e)(4)(H) because an exemption is being claimed for subsection (d), making these subsections not applicable.

(h) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(i) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment reporting on investigations and impede the development of intelligence necessary for effective law enforcement.

(j) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue search authorizations and could reveal investigative techniques and procedures.

(k) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

(l) From subsection (g) because portions of this system of records are compiled for law enforcement purposes and have been exempted from the access provisions of subsections (d) and (f).

p. System identifier: A0195-2a USACIDC.

(1) System name: Source Register.

(2) Exemption: (A): Portions of this system of records may be exempt pursuant to 5 USC 552a(j)(2) from subsections 5 USC 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g).

(3) Authority: 5 USC 552a(j)(2).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (c)(4) because an exemption is being claimed for subsection (d), making this subsection not applicable.

(c) From subsection (d) because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(d) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(e) From subsection (e)(2) because in a criminal investigation, the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection.

(f) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life and physical safety of confidential informants.

(g) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from access provisions of subsection (d), making these subsections not applicable.

(h) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(i) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment reporting on investigations and impede the development of intelligence necessary for effective law enforcement.

(j) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue search authorizations and could reveal investigative techniques and procedures.

(k) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

(l) From subsection (g) because portions of this system of records are compiled for law enforcement purposes and have been exempted from the access provisions of subsections (d) and (f).

q. System identifier: A0195-2b USACIDC.

(1) System name: Criminal Investigation and Crime Laboratory Files.

(2) Exemption: Portions of this system of records may be exempt pursuant to 5 USC 552a(j)(2) from subsections 5 USC 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g).

(3) Authority: 5 USC 552a(j)(2).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (c)(4) because an exemption is being claimed for subsection (d), making this subsection not applicable.

(c) From subsection (d) because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(d) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(e) From subsection (e)(2) because in a criminal or other law enforcement investigation, the requirement that information be collected to the greatest extent possible from the subject individual would alert the subject as to the nature or existence of the investigation and thereby present a serious impediment to effective law enforcement.

(f) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life and physical safety of confidential informants.

(g) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from access provisions of subsection (d), making these subsections not applicable.

(h) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(i) From subsection (e)(5) because the requirement that records be maintained with attention to accuracy, relevance, timeliness, and completeness would unfairly hamper the investigative process. It is the nature of law enforcement for investigations to uncover the commission of illegal acts at diverse stages. It is frequently impossible to determine initially what information is accurate, relevant, timely, and least of all complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light.

(j) From subsection (e)(8) because the notice requirements of this provision could present a serious impediment to criminal law enforcement by revealing investigative techniques, procedures, and the existence of confidential investigations.

(k) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

(l) From subsection (g) because portions of this system of records are compiled for law enforcement purposes and have been exempted from the access provisions of subsections (d) and (f).

r. System identifier: A0195-2c USACIDC DOD.

(1) System name: DOD Criminal Investigation Task Force (CITF) Files.

(2) Exemption: Portions of this system of records may be exempt pursuant to 5 USC 552a(j)(2) from subsections 5 USC 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g).

(3) Authority: 5 USC 552a(j)(2).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (c)(4) because an exemption is being claimed for subsection (d), making this subsection not applicable.

(c) From subsection (d) because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(d) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(e) From subsection (e)(2) because in a criminal or other law enforcement investigation, the requirement that information be collected to the greatest extent possible from the subject individual would alert the subject as to the nature or existence of the investigation and thereby present a serious impediment to effective law enforcement.

(f) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life and physical safety of confidential informants.

(g) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from access provisions of subsection (d), making these subsections not applicable.

(h) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(i) From subsection (e)(5) because the requirement that records be maintained with attention to accuracy, relevance, timeliness, and completeness would unfairly hamper the investigative process. It is the nature of law enforcement for investigations to uncover the commission of illegal acts at diverse stages. It is frequently impossible to determine initially what information is accurate, relevant, timely, and least of all complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light.

(j) From subsection (e)(8) because the notice requirements of this provision could present a serious impediment to criminal law enforcement by revealing investigative techniques, procedures, and the existence of confidential investigations.

(k) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

(l) From subsection (g) because portions of this system of records are compiled for law enforcement purposes and have been exempted from the access provisions of subsections (d) and (f).

s. System identifier: A0195-2d USACIDC DOD.

(1) System name: Defense Criminal Investigation DNA Database and Sample Repository; CODIS Records.

(2) Exemption: Portions of this system of records may be exempt pursuant to 5 USC 552a(j)(2) from subsections 5 USC 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g).

(3) Authority: 5 USC 552a(j)(2).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (c)(4) because an exemption is being claimed for subsection (d), making this subsection not applicable.

(c) From subsection (d) because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(d) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(e) From subsection (e)(2) because in a criminal investigation, the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection.

(f) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life and physical safety of confidential informants.

(g) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from the access provisions of subsection (d), making these subsections not applicable.

(h) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(i) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment reporting on investigations and impede the development of intelligence necessary for effective law enforcement.

(j) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue search authorizations and could reveal investigative techniques and procedures.

(k) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

(l) From subsection (g) because portions of this system of records are compiled for law enforcement purposes and have been exempted from the access provisions of subsections (d) and (f).

t. System identifier: A0195-6 USACIDC.

(1) System name: Criminal Investigation Accreditation and Polygraph Examiner Evaluation Files.

(2) Exemption: Portions of this system of records may be exempt pursuant to 5 USC 552a(k)(2), (k)(5), or (k)(7) from subsections 5 USC 552a (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f).

(3) Authority: 5 USC 552a(k)(2), (k)(5), and (k)(7).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (d), because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(c) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(d) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from the access provisions of subsection (d), making these subsections not applicable.

(e) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(f) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

u. System identifier: A0210-7 DAMO.

(1) System name: Expelled or Barred Person Files.

(2) Exemption: Portions of this system of records may be exempt pursuant to 5 USC 552a(j)(2) from subsections 5 USC 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(8), (f) and (g).

(3) Authority: 5 USC 552a(j)(2).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (c)(4) because an exemption is being claimed for subsection (d), making this subsection not applicable.

(c) From subsection (d) because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(d) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(e) From subsection (e)(2) because in a criminal investigation, the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection.

(f) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life and physical safety of confidential informants.

(g) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from the access provisions of subsection (d), making these subsections not applicable.

(h) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(i) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue search authorizations and could reveal investigative techniques and procedures.

(j) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

(k) From subsection (g) because portions of this system of records are compiled for law enforcement purposes and have been exempted from the access provisions of subsections (d) and (f).

v. System identifier: A0340-21 OAA.

(1) System name: Privacy Case Files.

(2) Exemption: During the processing of a Privacy Act request (which may include access requests, amendment requests, and requests for review for initial denials of such requests), exempt materials from other systems of records may in turn become part of the case record in this system. To the extent that copies of exempt records from those 'other' systems of records are entered into this system, the Department of the Army hereby claims the same exemptions.

(3) Authority: 5 USC 552a(j)(2), and (k)(1) through (k)(7)

(4) Reasons: Records are only exempt from pertinent provisions of 5 USC 552a to the extent such provisions have been identified and an exemption claimed for the original record and the purposes underlying the exemption for the original record still pertain to the record which is now contained in this system of records. In general, the exemptions were claimed in order to protect properly classified information relating to national defense and foreign policy, to avoid interference during the conduct of criminal, civil, or administrative actions or investigations, to ensure protective services provided to the President and others are not compromised, to protect records used solely as statistical records, to protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations, and to preserve the confidentiality and integrity of Federal evaluation materials. The exemption rule for

the original records will identify the specific reasons why the records may be exempt from specific provisions of 5 USC 552a.

w. System identifier: A0351-12 DAPE.

(1) System name: Applicants/Students, U.S. Military Academy Prep School.

(2) Exemption: (A) Portions of this system of records may be exempt pursuant to 5 USC 552a(k)(5) and (k)(7) subsections 5 USC 552a (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f).

(3) Authority: 5 USC 552a(k)(5) and (k)(7).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (d), because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(c) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(d) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from the access provisions of subsection (d), making these subsections not applicable.

(e) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(f) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

x. System identifier: A0351-17a USMA.

(1) System name: U.S. Military Academy Candidate Files.

(2) Exemption: Portions of this system of records may be exempt pursuant to 5 USC 552a(k)(5), (k)(6) or (k)(7) from subsections 5 USC 552a (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f).

(3) Authority: 5 USC 552a(k)(5), (k)(6) and (k)(7).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (d), because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(c) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(d) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from the access provisions of subsection (d), making these subsections not applicable.

(e) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(f) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

y. System identifier: A0351-17b USMA.

(1) System name: U.S. Military Academy Management System Records.

(2) Exemption: Portions of this system of records may be exempt pursuant to 5 USC 552a(k)(5) or (k)(7) from subsections 5 USC 552a (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f).

(3) Authority: 5 USC 552a(k)(5) and (k)(7).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (d), because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(c) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(d) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from the access provisions of subsection (d), making these subsections not applicable.

(e) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(f) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

z. System identifier: A0380-67 DAMI.

(1) System name: Personnel Security Clearance Information Files.

(2) Exemption: Portions of this system of records may be exempt pursuant to 5 USC 552a(k)(1), (k)(2), or (k)(5) from subsections 5 USC 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) Authority: 5 USC 552a(k)(1), (k)(2), or (k)(5).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (d), because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(c) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(d) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from the access provisions of subsection (d), making these subsections not applicable.

(e) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(f) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

aa. System identifier: A0381-20b DAMI.

(1) System name: Foreign Intelligence/Counterintelligence/Information Operations/Security Files

(2) Exemption: Portions of this system of records may be exempt pursuant to 5 USC 552a(k)(1), (k)(2) and (k)(5) from subsections 5 USC 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f)(E) To the extent that copies of exempt records from external systems of records are entered into A0381-10b DAMI, the Army hereby claims the same exemptions for those records as claimed for the original primary system of which they are a part.

(3) Authority: 5 USC 552a(j)(2), and (k)(1) through (k)(7).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (d), because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(c) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law

enforcement, it is necessary that this valuable information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(d) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from the access provisions of subsection (d), making these subsections not applicable.

(e) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(f) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

(g) For records that are copies of exempt records from external systems of records, such records are only exempt from pertinent provisions of 5 USC 552a to the extent such provisions have been identified and an exemption claimed for the original record and the purposes underlying the exemption for the original record still pertain to the record which is now contained in this system of records. In general, the exemptions were claimed in order to protect properly classified information relating to national defense and foreign policy, to avoid interference during the conduct of criminal, civil, or administrative actions or investigations, to ensure protective services provided to the President and others are not compromised, to protect records used solely as statistical records, to protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations, to preserve the confidentiality and integrity of Federal testing materials, and to safeguard evaluation materials used for military promotions when furnished by a confidential source. The exemption rule for the original records will identify the specific reasons why the records are exempt from specific provisions of 5 USC 552a.

*bb.* System identifier: A0381-100a DAMI.

(1) System name: Intelligence/Counterintelligence Source Files.

(2) Exemption: Portions of this system of records may be exempt pursuant to 5 USC 552a(k)(1), (k)(2), or (k)(5) from subsections 5 USC 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f).

(3) Authority: 5 USC 552a(k)(1), (k)(2), and (k)(5).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (d), because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(c) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(d) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from the access provisions of subsection (d), making these subsections not applicable.

(e) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(f) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

*cc.* System identifier: A0381-100b DAMI.

(1) System name: Technical Surveillance Index.

(2) Exemption: (A) Portions of this system of records may be exempt pursuant to 5 USC 552a(k)(1), (k)(2), or (k)(5) from subsections 5 USC 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f).

(3) Authority: 5 USC 552a(k)(1), (k)(2) or (k)(5).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (d), because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(c) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(d) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from the access provisions of subsection (d), making these subsections not applicable.

(e) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(f) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

*dd.* System identifier: A0600-20 DCS G-1.

(1) System name: Sexual Assault (SADMS) and sexual harassment/assault response and prevention (SHARP) Program Records.

(2) Exemptions: This system of records is a compilation of information from other Department of Defense/Army systems of records. To the extent that copies of exempt records from those other systems of records are entered into this system of records, the Army G-1 hereby claims the same exemptions for the records from those other systems.

(3) Authority: 5 USC 552a(j)(2), and (k)(1) through (k)(7).

(4) Reasons: Records are only exempt from pertinent provisions of 5 USC 552a to the extent such provisions have been identified and an exemption claimed for the original record and the purposes underlying the exemption for the original record still pertain to the record which is now contained in this system of records. In general, the exemptions were claimed in order to protect properly classified information relating to national defense and foreign policy, to avoid interference during the conduct of criminal, civil, or administrative actions or investigations, to ensure protective services provided to the President and others are not compromised, to protect records used solely as statistical records, to protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations, to preserve the confidentiality and integrity of Federal testing materials, and to safeguard evaluation materials used for military promotions when furnished by a confidential source. The exemption rule for the original records will identify the specific reasons why the records may be exempt from specific provisions of 5 USC 552a.

*ee.* System identifier: A0601-141 DASG.

(1) System name: Applications for Appointment to Army Medical Department.

(2) Exemption: Portions of the system of records may be exempt pursuant to 5 USC 552(a)(k)(5) from subsections 5 USC 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f).

(3) Authority: 5 USC 552a(k)(5).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (d), because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(c) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(d) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from the access provisions of subsection (d), making these subsections not applicable.

(e) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(f) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

*ff.* System identifier: A0601-210a USAREC.

(1) System name: Enlisted Eligibility Files.

(2) Exemption: Portions of this system of records may be exempt pursuant to 5 USC 552a(k)(5) from subsections 5 USC 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f).

(3) Authority: 5 USC 552a(k)(5).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (d), because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(c) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(d) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from the access provisions of subsection (d), making these subsections not applicable.

(e) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(f) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

*g.g.* System identifier: A0601-222 USMEPCOM.

(1) System name: Armed Services Military Accession Testing.

(2) Exemption: Portions of the system of records may be exempt pursuant to 5 USC 552a(k)(6), from subsection 5 USC 552a(d).

(3) Authority: 5 USC 552a(k)(6).

(4) Reasons: An exemption is required for those portions of the Skill Qualification Test system pertaining to individual item responses and scoring keys to preclude compromise of the test and to ensure fairness and objectivity of the evaluation system.

*h.h.* System identifier: A0608-18 DASG.

(1) System name: Army Family Advocacy Program Files.

(2) Exemptions: Portions of the system of records may be exempt pursuant to 5 USC 552a(k)(2) or (k)(5) from subsections 5 USC 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) Authority: 5 USC 552a(k)(2) and (k)(5).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (d) because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(c) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(d) From subsections (e)(4)(G) and (e)(4)(H) because the requirements in those subsections are inapplicable to the extent that portions of this system of records may be exempt from subsection (d), concerning individual access.

(e) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(f) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

*i.i.* System identifier: A0614-115 DAMI.

(1) System name: Department of the Army Operational Support Activities.

(2) Exemption: Portions of this system of records may be exempt pursuant to 5 USC 552a(k)(1), (k)(2), or (k)(5) from subsections 5 USC 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) Authority: 5 USC 552a(k)(1), (k)(2), and (k)(5).

(4) Reasons:

(a) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(b) From subsection (d), because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(c) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(d) From subsections (e)(4)(G) and (e)(4)(H) because portions of this system of records have been exempted from the access provisions of subsection (d), making these subsections not applicable.

(e) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(f) From subsection (f) because portions of this system of records have been exempted from the access provisions of subsection (d).

## **C-2. Exempt Office of Personnel Management records**

Three Office of Personnel Management systems of records apply to Army employees, except for non-appropriated fund employees. These systems, the specific exemptions determined to be necessary and proper, the records exempted, provisions of the Privacy Act from which exempt, and justification are set forth in the following paragraphs.

### *a. Personnel Investigations Records (OPM/CENTRAL-9).*

(1) Exemptions: Portions of this system of records may be exempt pursuant to 5 USC 552a(k)(1), (k)(2), (k)(3), (k)(5), (k)(6), or (k)(7) from subsections 5 USC 552a(c)(3) and (d).

#### (2) Reasons:

(a) Personnel investigations may obtain from another Federal agency, properly classified information which pertains to national defense and foreign policy. Application of exemption (k)(1) may be necessary to preclude the data subject's access to an amendment of such classified information under 5 USC 552a(d) in order to protect such information.

(b) Personnel investigations may contain investigatory material compiled for law enforcement purposes other than material within the scope of 5 USC 552a(j)(2), for example, investigations into the administration of the merit system. Application of exemption (k)(2) may be necessary to preclude the data subject's access to or amendment of such records, under 552a(c)(3) and (d) because otherwise, it would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(c) Personnel investigations may obtain, from another Federal agency, information that relates to providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18. Application of exemption (k)(3) may be necessary to preclude the data subject's access to or amendment of such records under 5 USC 552a(d) to ensure protective services provided to the President and others are not compromised.

(d) All information about individuals in these records that meets the criteria stated in 5 USC 552a(k)(5) is exempt from the requirements of 5 USC 552a(c)(3) and (d) in order to protect the identity of confidential sources incident to determinations of suitability, eligibility, or qualifications for Federal employment, military service, contract, and security clearance determinations.

(e) All material and information in the records that meets the criteria stated in 5 USC 552a(k)(6) is exempt from the requirements of 5 USC 552a(d), relating to access to and amendment of records by the data subject in order to preserve the confidentiality and integrity of Federal testing materials.

(f) All material and information in the records that meets the criteria stated in 5 USC 552a(k)(7) is exempt from the requirements of 5 USC 552a(d), relating to access to and amendment of records by the data subject in order to safeguard evaluation materials used for military promotions when furnished by a confidential source.

### *b. Recruiting, Examining, and Placement Records (OPM/GOVT-5).*

#### (1) Exemptions:

(a) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 USC 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(b) Testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service may be exempt pursuant to 5 USC 552a(k)(6), if the disclosure would compromise the objectivity or fairness of the test or examination process.

(c) Therefore, portions of this system of records may be exempt pursuant to 5 USC 552a(k)(5), or (k)(6) from subsections 5 USC 552a(c)(3) and (d).

(2) Reasons:

(a) All information about individuals in these records that meets the criteria stated in 5 USC 552a(k)(5) is exempt from the requirements of 5 USC 552a(c)(3) and (d) in order to protect the identity of confidential sources incident to determinations of suitability, eligibility, or qualifications for Federal employment, military service, contract, and security clearance determinations. These exemptions are also claimed because this system contains investigative material compiled solely for the purpose of determining the appropriateness of a request for approval of an objection to an eligible individual's qualification for employment in the Federal service.

(b) All material and information in these records that meets the criteria stated in 5 USC 552a(k)(6) are exempt from the requirements of 5 USC 552a(d), relating to access and amendment of records by the subject, in order to preserve the confidentiality and integrity of Federal testing materials.

c. Personnel Research Test Validation Records (OPM/GOVT-6).

(1) Exemptions: Testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service may be exempt pursuant to 5 USC 552a(k)(6), if the disclosure would compromise the objectivity or fairness of the test or examination process. Therefore, portions of this system of records may be exempt pursuant to 5 USC 552a(k)(6) from subsection 5 USC 552a(d).

(2) Reasons: All material and information in these records that meets the criteria stated in 5 USC 552a(k)(6) is exempt from the requirements of 5 USC 552a(d), relating to access to an amendment of the records by the data subject, in order to preserve the confidentiality and integrity of Federal testing materials.

## Appendix D

### Privacy Act Statement

#### D-1. Usage

Provide a PAS to individuals when information is collected that will be maintained in a Privacy Act system of records, regardless of the medium used to collect the information (for example, forms, personal interviews, telephonic interviews, and other methods). Also provide a PAS when individuals are asked to confirm that their data is current and correct.

#### D-2. Elements

The elements of a PAS include AUTHORITY, PRINCIPAL PURPOSE, ROUTINE USES, and DISCLOSURE. Figure D-1 describes each element.

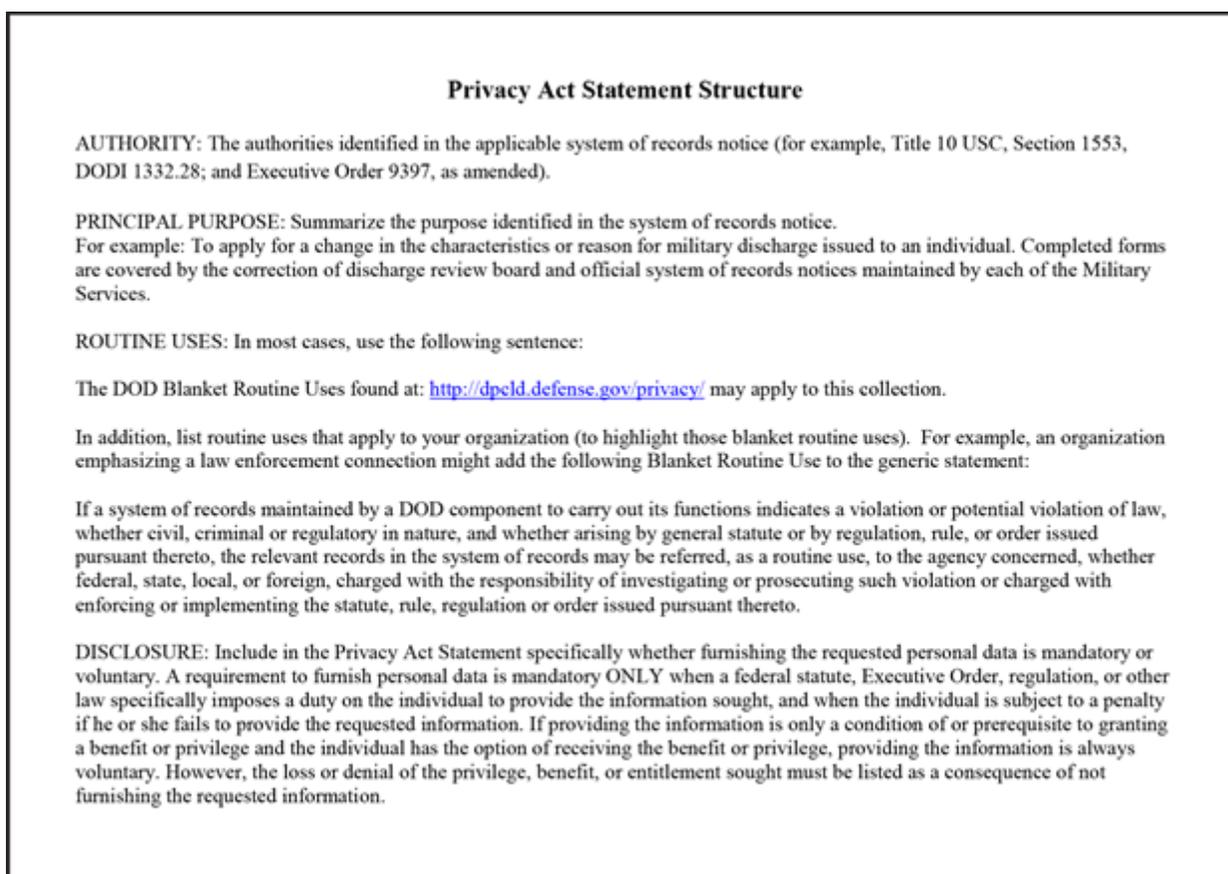


Figure D-1. Privacy Act Statement Structure

## **Appendix E**

### **System of Records Notice Samples**

Actual documents will vary widely based on the responsible organization and the characteristics of the system of records notice.

#### **E-1. Sample of System of Records Notice**

Figure E-1 provides a sample system of records notice.

## **United States Army**

A0600-8b AHRC (system identifier)

### **SYSTEM NAME:**

Soldiers' Criminal History Files (FR May 7, 2013, Volume 78, Page 26623).

### **SYSTEM LOCATION:**

At each Brigade-level or higher Command. Official mailing addresses are published as an appendix to the Army's compilation of systems of records notices.

### **CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

Active duty, National Guard and Reserve commissioned officers, warrant officers and enlisted personnel assigned or projected for assignment to Army units.

### **CATEGORIES OF RECORDS IN THE SYSTEM:**

Reports of Soldiers with criminal convictions and investigations included in the report information from witnesses, victims that resulted in founded offenses over the preceding 5-year period and related documentation. Information in the reports includes: Soldier's name, Social Security Number (SSN), rank, aliases, date, location, and description of the offense; case number of the reported offense, Department of the Army Form 4833, Commander's Report of Disciplinary or Administrative Action, Department of the Army Form 3975, Military Police Reports-MPRs, and adjudication of the founded offense as guilty, not guilty or unknown. If a Soldier has no criminal history within the preceding 5-year period, the report will show a negative entry.

### **AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

10 U.S.C. 3013, Secretary of the Army; AR 27-10, Military Justice; AR 25-2, Information Assurance; AR 600-8, Military Human Resources Management; AR 600-20, Army Command Policy; Army Directive 2013-06, Providing Specific Law Enforcement Information to Commanders of Newly Assigned Soldiers; and Executive Order 9397 (SSN), as amended.

### **PURPOSE(S):**

This system will give Brigade-level or higher commanders an additional tool to help them promote the health, resilience, well-being and readiness of their Soldiers by ensuring command awareness of Soldiers who have engaged in potentially high-risk criminal behaviors. Provides commanders the information they need to take appropriate intervention measures such as referral for counseling, treatment and assistance, as required to mitigate potential risks. Brigade-level or higher Commander may further disclose information from the files only to those with an official need to know.

### **ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:**

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, these records contained therein may specifically be disclosed outside the DOD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

The DOD Blanket Routine Uses set forth at the beginning of the Army's compilation of systems of records notices may apply to this system.

Figure E-1. Example of a System of Records Notice

**POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:**

**STORAGE:**

Paper records and electronic storage media.

**RETRIEVABILITY:**

By name, SSN and rank.

**SAFEGUARDS:**

Records are protected by physical security devices, computer hardware and software safeguard features, and restrictions on system access to only those personnel with an official need to know.

Soldiers' Criminal History Files will be sent via authorized government electronic mail with Public Key Infrastructure (PKI) encryption only to the Brigade-level or higher Commander who may further disclose information from the files to those with an official need to know. Personnel with an official need to know include individuals with responsibility for risk assessment and management, such as the chain of command, brigade judge advocate, paralegal noncommissioned officer, and administrative personnel.

Paper records are stored in secure container/file cabinets with access restricted to Brigade-level or higher commanders and personnel with an official need to know.

**RETENTION AND DISPOSAL:**

Soldier's Criminal history reports sent to commanders are deleted or destroyed by shredding after the Soldier departs the unit.

**SYSTEM MANAGER(S) AND ADDRESS:**

U.S. Army Human Resources Command, Deputy G-3 Operations (HRC-PL), 1600 Spearhead Division Avenue (1-3-021), Ft Knox, KY 40122-5102.

**NOTIFICATION PROCEDURE:**

Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to the Brigade-level or higher Commander of the unit to which the Soldier is assigned or the designated representative of the Commander. Official mailing addresses are published as an appendix to the Army's compilation of systems of records notices.

The request should provide their full name, SSN, current address, and sufficient details to permit locating pertinent records.

**RECORD ACCESS PROCEDURES:**

Individuals seeking access to information about themselves contained in this system should address written inquiries to the Army activity to which the gift or donation was submitted. If unsure you may submit to Office of the Administrative Assistant to the Secretary of the Army.

The request should provide their full name, SSN, current address, and sufficient details to permit locating pertinent records.

**CONTESTING RECORD PROCEDURES:**

The Army's rules for accessing records, and for contesting contents and appealing initial agency determinations are contained in Army Regulation 25-XX; 32 CFR 505; or may be obtained from the system manager.

Figure E-1. Example of a System of Records Notice—continued

---

**RECORD SOURCE CATEGORIES:**  
Subjects of criminal investigations, witnesses, victims, Military Police and U.S. Army Criminal Investigation Command personnel and special agents, informants, various Department of Defense, federal, state and local investigative and law enforcement agencies, departments or agencies of foreign governments, and any other individuals or organizations that may supply pertinent information.

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**  
None.

---

Figure E-1. Example of a System of Records Notice—continued

## E-2. Sample of Completion Checklist

Figure E-2 provides a system of records notice checklist.

### Army System of Records Notice Checklist

1. **System identifier:** The system identifier is an alphanumeric descriptor with the leading character of "A" indicating the Army component. The Army Privacy Office assigns the identifier for a new system of records notice (for example, A0190-45 OPMG).
2. **System name:** The system name reflects the categories of individuals on whom information is maintained (for example, Army Science Board (ASB)).
3. **System location:** The system location is the complete mailing address of each site maintaining the system of records, including the 9-digit ZIP code.
4. **Categories of individuals covered by the system:** Reflects the categories of individuals about whom records are maintained so that individuals can determine if system records exist for them.
5. **Categories of records in the system:** Contains a description of the types of personally identifiable information which are maintained in the system (for example, Social Security Number, DOD ID number, date of birth, patient medical history, loan applications, or laboratory test results).
6. **Authority for maintenance of the system:** States the specific legal authority (citation and descriptive title) for maintenance of the system (for example, Statute, Executive Order, or Army regulation).
7. **Purpose:** States the Army purpose for which the system of records was established and uses of the information.
8. **Routine uses of records maintained in the system, including categories of users and purposes of use:** Lists each authorized routine use of the information outside the Army. Each individual routine use identifies the third party, to whom disclosure is authorized, the type of information, and purpose for the disclosure.
9. **Disclosure to consumer reporting agencies:** (Entry is optional). Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system.
10. **Storage:** Describes the storage media for the records (for example, file folders, file cabinets, or electronic media).
11. **Retrievability:** States how individual records are retrieved from the system (for example, by name, SSN, or other personal identifier).
12. **Safeguards:** Describes all measures currently in place to minimize the risk of unauthorized access to or disclosure of records in the system, reflecting the most recent risk analysis; also identifies the categories of employees authorized to have access to the records.
13. **Retention and disposal:** States the length of time records are maintained by the Component in an active status, when they are transferred to a Federal records center, how long they are kept at the Federal records center, and when they are transferred to the National Archives or destroyed. If records are eventually to be destroyed, state the method of destruction (for example, shredding, burning, or pulping).
14. **System manager and address:** States the title (not the individual's name) and current address (including 9-digit ZIP code) of the Army official responsible for the system's policies and practices.
15. **Notification procedure:** Describes how an individual can determine if and how a record in the system of records applies. Includes the title and complete mailing address of the official to whom the request must be directed, the information the individual must provide in order for the Army to respond to the request, and a description of any proof of identify required.
16. **Record access procedures:** Describes how an individual can review the record or obtain a copy of it. Provides the title and complete mailing address of the official to whom the request for access must be directed, the information the individual must provide in order for the Army to respond to the request, and a description of any proof of identity required.
17. **Contesting record procedures:** This entry should read the same for all Army notices: "The Army's rules for accessing records, and for contesting contents, are contained in Army Regulation 25-XX, 32 CFR 505, or can be obtained from the system manager."
18. **Record source categories:** Describes where the Army obtained the information (source documents and other agencies) maintained in the system; describes the record sources in general terms.
19. **Exemptions claimed for the system:** If no exemption has been established for the system, the section indicates "None." If any exemption rule has been established, this section states under which provision of the Privacy Act it was established. Also, that an exemption rule has been promulgated in accordance with the requirements of 5553(b)(1), (2), and (3), (c) and (e).

Figure E-2. Army System of Records Notice Checklist

### **E-3. Sample of Narrative Statement**

Figure E-3 provides a sample narrative statement.

## SAMPLE/Instructions only

DEPARTMENT OF DEFENSE

Department of the Army

Narrative Statement on a New or Altered System of Records

Under the Privacy Act of 1974

(Must use Courier New Font Size 12)

1. **System identifier and name:** Provide system identifier and system name.
2. **Responsible official:** Full name, address and telephone number of individual who can best answer questions regarding this system of records.
3. **Purpose of establishing the system:** This entry should read same as in the notice.  
When submitting an alteration, this entry will read "Nature of the changes proposed for the system:"  
An alteration consists of one or more of the following:
  1. A significant increase in the number, type, or category of individuals about whom records are maintained.
  2. A change that expands the types or categories of information maintained.
  3. A change that alters the purpose for which the information is used.
  4. A change to equipment configuration (either hardware or software) that creates substantially greater access to the records in the system of records.
  5. Addition of an exemption.
  6. Addition of a routine use.
4. **Authority for the maintenance of the system:** This entry should read the same as in the notice.
5. **Provide the agencies evaluation on the probable or potential effects on the privacy of individuals:**  
OMB does not provide any guidance as to what they expect under this entry. However, the Defense Privacy and Civil Liberties Division (DPCLD) is looking for any known or perceived adverse effects on the individual by maintaining this information. Typically this entry reads "None".
6. **Is the system, in whole or in part, being maintained, collected, used or disseminated by a contractor?** This entry is either YES or NO. If YES, please ensure that the contract has the necessary FAR clauses (subpart 24.1).
7. **Steps taken to minimize risk of unauthorized access:**  
Briefly describe the steps taken to minimize the risk of unauthorized access. Agency must have performed a risk assessment upon establishing a new system of records. Last sentence will read "A risk assessment has been performed and will be made available on request." Make sure that a

Figure E-3. Army System of Records Notice Narrative Statement

risk assessment has been performed for all new systems of records. Army Privacy does not collect risk assessments.

8. **Routine use compatibility:**

This is an example of the standard blurb. Of course, if the Blanket Routine Uses (BRUs) do not apply, we would not use the last sentence in the standard blurb.

9. **OMB information collection requirements:**

This is required when you are collecting information from the public to be maintained in the system of records. (Contact the Army's Information Management Control Officer (IMCO) in the Army Records Management Division if you have any questions.

OMB collection required: Yes/No

OMB Control Number:

Date submitted to OMB:

Expiration Date:

If No, then state reason:

10. **Name of IT system (state NONE if paper records only):**

(If the collection is on paper records only, put NONE; if the collection is electronic, enter the name of the electronic system.)

Figure E-3. Army System of Records Notice Narrative Statement—continued

## Appendix F

### Internal Control Evaluation

#### F–1. Function

The function covered by this evaluation is the Army Privacy Program.

#### F–2. Purpose

The purpose of this evaluation is to assist users of AR 25–22 in evaluating the key internal controls listed. It is not intended to cover all controls.

#### F–3. Instructions

Answers must be based on the actual testing of key internal controls (for example, document analysis, direct observation, sampling, and simulation). Answers that indicate deficiencies must be explained and the corrective action identified in supporting documentation. These internal controls must be evaluated at least once every five years. Certification that the evaluation has been conducted must be accomplished on DA Form 11–2 (Internal Control Evaluation Certification).

#### F–4. Test questions

- a.* Is a Privacy Act Program established and implemented in your organization?
- b.* Is an individual appointed to implement the Privacy requirements?
- c.* Are appointed privacy officials providing annual privacy training tailored to their organization requirement?
- d.* Are privacy officials providing to Army Privacy Office all reports mandated by law (annual Federal Information Security Management Act of 2002, quarterly Public Law 110–53, Sec. 803 and OMB Circular A–130, appendix I)
- e.* When more than 30 calendar days are required to respond, is the Privacy Act requester informed, explaining the circumstance requiring the delay and provided an appropriate date for completion?
- f.* Are System of Records Notices posted in the FR reviewed by the system owners every two years and reported through their privacy official to the APO?
- g.* Are accounting disclosure logs being maintained?

#### F–5. Supersession

Not applicable.

#### F–6. Comments

Help make this a better tool for evaluating internal controls. Submit comments to the Army Privacy Office via the e-mail address specified at: <https://www.rmda.army.mil/privacy/rmda-po-contact.html> or via U.S. Mail to the Records Management and Declassification Agency, 7701 Telegraph Road, Casey Building, Room 102, Alexandria, VA 22315-3827.

## **Glossary**

### **Section I**

#### **Abbreviations**

**AAFES**

Army and Air Force Exchange Service

**AASA**

Administrative Assistant to the Secretary of the Army

**ACOM**

Army command

**AFI**

Air Force Instruction

**AKO**

Army Knowledge Online

**APD**

Army Publishing Directorate

**APO**

Army Privacy Office

**ARIMS**

Army Records Information Management System

**ASCC**

Army service component commands

**BPA**

Blanket Purchase Agreement

**CFR**

Code of Federal Regulations

**CITF**

Criminal Investigation Task Force

**CONUS**

continental United States

**DA**

Department of the Army

**DAJA**

Department of the Army, Judge Advocate General

**DAMI**

Department of the Army, Military Intelligence

**DASG**

Department of the Army, Surgeon General

**DD**

Department of Defense

**DNA**

deoxyribonucleic acid

**DOD**

Department of Defense

**DODD**

Department of Defense directive

**DODI**

Department of Defense instruction

**DPCLD**

Defense Privacy and Civil Liberties Division

**DRU**

direct reporting unit

**EEO**

Equal Employment Opportunity

**FAR**

Federal Acquisition Regulation

**FIPPS**

fair information practice principles

**FOIA**

Freedom of Information Act

**FOIA/PA**

Freedom of Information Act and Privacy Act

**FOUO**

for official use only

**FR**

Federal Register

**FTC**

Federal Trade Commission

**GSA**

General Services Administration

**HIPAA**

Health Insurance Portability and Accountability Act

**HQDA**

Headquarters, Department of the Army

**IA**

information assurance

**ID**

identification data

**KM**

knowledge management

**NARA**

National Archives and Records Administration

**NIST**

National Institute of Standards and Technology

**OAA**

Office of the Administrative Assistant

**OAASA**

Office of the Administrative Assistant to the Secretary of the Army

**OMB**

Office of Management and Budget

**OPM**

Office of Personnel Management

**OPMG**  
Office of the Provost Marshal General

**OTJAG**  
Office of the Judge Advocate General

**PA**  
Privacy Act

**PAA**  
Privacy Act Advisory

**PAS**  
Privacy Act Statement

**PATS**  
Privacy Act Tracking System

**PDF**  
portable document format

**PHI**  
protected health information

**PIA**  
privacy impact assessment

**PII**  
personally identifiable information

**PKI**  
Public Key Infrastructure

**PMG**  
Provost Marshal General

**RMDA**  
Records Management and Declassification Agency

**SADMS**  
Sexual Assault Data Management System

**SAIG**  
Inspector General of the Army

**SAOP**  
senior agency official for privacy

**SF**  
Standard Form

**SHARP**  
sexual harassment/assault response and prevention

**SOR**  
system of records

**SORN**  
system of record notice

**SSN**  
Social Security Number

**TJAG**  
The Judge Advocate General

**USACIDC**  
U.S. Army Criminal Investigation Command

**USAR**

U.S. Army Reserve

**USAREC**

U.S. Army Recruiting Command

**USC**

United States Code

**US-CERT**

U.S. Computer Emergency Readiness Team

**USMA**

U.S. Military Academy

**USMEPCOM**

U.S. Military Entrance Processing Command

**Section II****Terms****Access**

The review of a record or the process of obtaining a copy of an entire record or part of a record that holds personally identifiable information.

**Adequate Security**

Security commensurate with the risk and magnitude of the potential harm resulting from loss, misuse, or unauthorized access to PII. This includes providing adequate and appropriate confidentiality, integrity, and availability.

**Agency**

The DOD is a single agency for the purpose of disclosing records subject to The Privacy Act of 1974. For other purposes, including access, amendment, appeals from denials of access or amendment, exempting systems of records, and record-keeping for release to non-DOD agencies, the DA is also an agency.

**Amendment**

The process of adding, deleting, or changing information in a record thus revising the data to timely, accurate, complete, and relevant.

**Army Knowledge Online**

AKO is the U.S. Army's main intranet portal for knowledge management and information exchange. AKO includes an unclassified intranet and a more restricted intranet containing classified information. The main AKO intranet serves millions of registered users, including active duty and retired service personnel and their family members. AKO provides single sign-on access to applications and services.

**Army Records Information Management System**

A system for identifying, arranging, and retrieving Army records for reference and disposition according to the directive, usually an AR or DA pamphlet, which prescribes their creation, maintenance, and use.

**Biometric data**

A general term referring to individual traits, or identifiers, including a wide range of physical attributes, such as deoxyribonucleic acid (DNA), fingerprints and palm print, retinal and iris scans, full face photographs and scans, or an individual's behavioral attributes, such as voice pattern (signature), signature recognition (handwriting), and keystroke dynamics that are used to describe a characteristic or a process. In other words, biometric data can be a characteristic or a process. A characteristic: The measure of a biological (anatomical and physiological) or behavioral biometric trait that can be used for automated recognition. A process: Automated methods of recognizing an individual based on the measure of biological (anatomical and physiological) or behavioral biometric characteristics.

**Breach**

Actual or suspected loss of control, unauthorized disclosure, or unauthorized access to PII, where persons other than authorized users gain access or potential access to such information for other than authorized purposes, where one or more individuals might be adversely affected.

**Code of Fair Information Practice**

According to the Code of Fair Information Practice, automated personal data systems must provide for collection protection, disclosure permission, secondary usage restrictions, record correction, and data security.

**Component**

A Military Service, Agency, or Field Activity within DOD.

**Computer Matching Agreement**

A written accord that establishes the conditions, safeguards, and procedures under which a Federal organization agrees to disclose data for a computerized comparison of two or more automated systems of records (for example, to verify eligibility for benefits payments or to recover delinquent debts).

**Confidential source**

A person or organization that has furnished information to the Government under an express promise that the person's or the organization's identity would be withheld.

**Contractor**

Any individual or other legal entity that directly or indirectly (for example, through an affiliate) conducts business or reasonably may be expected to conduct business with the U.S. Government as an agent or representative of another contractor via a contract for carriage under Government or commercial bills of lading, or a subcontract under a Government contract.

**Cookie**

Data on a Web server used to identify users and their preferences. Cookies are either persistent or third-party. A persistent cookie resides on a computer's hard drive. A third-party cookie operates on a Web site.

**Copy**

A reproduction or duplication of an original record. Copies identified by their function include action copy, file or record copy, reading copy, reference copy, and official copy. Copies identified by method of creation include carbon, electronic (pdf), offset printing, and microfiche. In electronic records, the action or result of reading data from a source leaves the source data unchanged and writes the same data elsewhere on a medium that may differ from the source.

**Cyber incident**

A cyber breach incident is related to computers, information networks, or communication systems. In contrast, a non-cyber breach incident is paper-based without a relationship to the abovementioned technical elements.

**Data subject**

The individual about whom the Army is maintaining information in a system of records.

**Defense Data Integrity Board**

Composed of representatives from DOD components and the services that oversee, coordinate, and approve all DOD computer matching programs covered by the Privacy Act.

**Denial authority**

The Army Staff agency head or Army commander with designated authority to deny access to, or refuse amendment of, records in an assigned area or functional specialization. An official granted authority to withhold records from an individual requested pursuant to the Privacy Act when: (1) The U.S. Army head maintaining a system of records has claimed an exemption according to sections (j) and (k) of the Privacy Act; and (2) The U.S. Army has established an exemption rule in the Federal Register.

**Disclosure**

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

**High risk breach**

A high risk breach is one that requires notification based on a balanced assessment of the factors of nature of the data elements breached, number of individuals affected, the likelihood that the breached data is accessible and usable, the likelihood that the breach may lead to harm, and the ability of the Army command to mitigate the risk of harm.

**Identity Theft or Misuse**

Identity theft usually involves the theft of credit card account numbers and the illicit use of those accounts. Misuse of personally identifiable information sometimes involves the unauthorized use of the identity of living or deceased individuals for deceitful purposes such as erroneous political campaign contributions.

**Incident**

A Privacy Incident is any potential or actual compromise of personally identifiable information (PII) in a form that could be accessed by an unauthorized person. The Government has characterized privacy incidents to include the 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.

**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 may also act on behalf of an individual. Members of the Military Services are individuals. Corporations, partnerships, sole proprietorships, professional groups, businesses, and other commercial entities are not individuals when acting in an entrepreneurial capacity with the Army, but are individuals when acting in a personal capacity (for example, security clearances, entitlement to specified privileges or benefits).

**Individual access**

Access to information pertaining to an individual by the individual, or by designated agent or legal guardian.

**Info Dissemination**

Information dissemination, within the context of PATS, is a general term for information retrieval (“pull”) from an internet or intranet system; email is a “push” method of disseminating information (sending). Info dissemination, for the purposes of PATS dissemination, relies upon a reader retrieving information.

**Information in Identifiable Form**

Information in an IT system or online collection that directly identifies an individual (for example, name, address, Social Security Number, DOD ID, telephone number, or email address) or indirectly identifies specific individuals along with other data elements (in other words, indirect identification may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

**Knowledge Management**

A discipline that promotes an integrated approach to identifying, retrieving, evaluating, and sharing an enterprise’s tacit and explicit knowledge assets to meet mission objectives. The objective is to connect those who know with those who need to know (know-why, know-what, know-who, and know-how) by leveraging knowledge transfers from one-to-many across the enterprise.

**Maintain**

The collection, maintenance, use, or dissemination of records contained in a system of records.

**Metadata**

Metadata is structured information that describes or otherwise makes it easier to retrieve, use, or manage an information resource. Metadata is often called data about data or information about information. Metadata does not normally contain PII.

**Minor**

A minor is an individual under 18 years of age, who is not a member of the U.S. Army, or married. Minors of interest to this regulation are usually children or legal dependents of U.S. Army members; dependents are not necessarily minors.

**Official use**

When Army personnel or contractors have demonstrated a need for the use of any record or the information contained therein in the performance of their official duties.

**Personally identifiable information**

Information which can be used to distinguish or trace an individual’s identity, such as name, Social Security Number, DOD ID, and biometric records, alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, and mother’s maiden name.

**Potential impact**

An actual or suspected breach of PII or PHI could have a limited adverse effect (low risk), a serious adverse effect (moderate risk), or a severe or catastrophic adverse effect (high risk) on organizational integrity or individual privacy.

**Privacy Act request**

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

**Privacy Act Statement**

A document that explains why the Army is collecting personal information, the purpose of the collection, and the consequences of not providing the requested information. A Privacy Act Statement is required when the collected personal information (name, date of birth, SSN, and so forth) will be entered into an Army system of records. This applies to all collection methods including forms, as well as personal and telephonic interviews.

**Privacy impact assessment**

An analysis of how personal information is handled to: (a) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (b) determine the risks and effects of collecting, maintaining, and disclosing personal information; and (c) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. The PIA process provides a way to ensure compliance with laws and regulations governing privacy.

**Protected health information**

Individually identifiable health information that relates to the individual's past, present, or future physical or mental health, the provision of health care, or the payment of health services, and that identifies the individual or it is reasonable to believe the information can be used to identify the individual.

**Record**

Any item, collection, or grouping of information about an individual that— (1) Is kept by the Government including an individual's home address, home telephone number, Social Security Number, education, financial transactions, medical history, and criminal or employment history; and (2) Contains an individual's name, identifying number, symbol, or other individual identifier such as a finger or voice print, or a photograph. Records should always be timely, accurate, complete, and relevant. Any item, collection, or grouping of information, whatever the storage media (for example, paper, electronic), about an individual that is maintained by the U.S. Army may be considered a record; this includes an individual's education, financial transactions, medical, criminal or employment history; and that contains the individual's name, or an identifying number, symbol, or other identifying particular assigned to the individual as described above.

**Records management**

The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the U.S. Army and effective and economical management of DA operations.

**Risk assessment**

An analysis considering information sensitivity, vulnerabilities, and cost in safeguarding PII processed or stored in the facility or activity.

**Routine use**

Disclosure of a record outside the U.S. Army without the consent of the subject individual for a use that is compatible with the purpose for which the information was collected and maintained by DA. The routine use must be included in the published system notice for the system of records involved.

**Statistical record**

A record maintained only for statistical research or reporting purposes and not used in whole or in part in making determinations about specific individuals.

**Substitute notice**

In a case where insufficient or out-of-date contact information precludes written notification to an affected individual, a substitute form of notice reasonably calculated to reach the potentially impacted individual shall be provided.

**System manager**

The privacy official responsible for policies and procedures for operating and safeguarding a system of records.

**System of records**

A group of records, whatever the storage media (paper, electronic, and so forth), under the control of a DA activity from which personal information about an individual is retrieved by the name of the individual, or by an identifying number, symbol, or other identifying particular assigned, that is unique to the individual. (A grouping of files or series of records

arranged chronologically or subjectively that is not retrieved by individual identifier is not a system of records, even though individual information could be retrieved by such an identifier, such as through a paper-by-paper search.)

**System of records notice**

A description of any Privacy Act system of records. System of records notices generally describe the “who, what, where, and why” of a system and describe the processes for individuals to access or contest the information being held on them in that system. These notices are required to be published in the Federal Register for a period of public comment before the system data collection (paper-based or electronic) is started. A system of records notice governed by this regulation is either maintained by the U.S. Army or by a Federal agency for a Government-wide program for which the Federal agency has responsibility in overseeing and directing as required by The Privacy Act (for example, OPM, GOVT-1, and general personnel records).

**Unique identification**

A system of establishing globally unique identifiers within DOD, and serves to distinguish a discrete entity or relationship from other like or unlike entities or relationships.

**Unique identifier**

A character string, number, or sequence of bits assigned to a discrete entity or its associated attribute, and serves to uniquely distinguish it from other like and unlike entities. Each unique identifier has only one occurrence within its defined scope of use.

**Web site**

A location on the Internet. All Web sites are referenced using a special addressing scheme called a Uniform Resource Locator. A Web site can mean a single Hypertext Markup Language file or hundreds of files placed on the Internet by an enterprise.

**Section III**

**Special Abbreviations and Terms**

This section contains no entries.

**UNCLASSIFIED**

**PIN 200925-000**