DEPARTMENT OF DEFENSE

Department of the Army

32 CFR Part 505

RIN 0702–AA53

[Docket No. USA–2006–0011]

The Army Privacy Program

AGENCY: Department of the Army, DoD.

ACTION: Final rule.

SUMMARY: The Department of the Army is updating policies and responsibilities for the Army Privacy Program, which implements the Privacy Act of 1974, by showing organizational realignments and by revising referenced statutory and regulatory authority, such as the Health Insurance Portability and Accountability Act and E-Government Act of 2002. This rule finalizes the proposed rule that was published in the **Federal Register** on April 25, 2006.

DATES: *Effective Date:* September 11, 2006.

ADDRESSES: U.S. Army Records Management and Declassification Agency, Freedom of Information and Privacy Office, 7701 Telegraph Road, Casey Bldg., Suite 144, Alexandria, VA 22315–3905.

FOR FURTHER INFORMATION CONTACT: Ms. Janice Thornton at (703) 428–6503.

SUPPLEMENTARY INFORMATION:

A. Background

In the April 25, 2006, issue of the **Federal Register** (71 FR 24494), the Department of the Army issued a proposed rule to revise 32 CFR part 505. It incorporates Privacy Act policy objectives to include (1) restricting disclosure of personally identifiable records maintained; (2) to grant individuals rights of access to agency records maintained on themselves; (3) to grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete; and (4) to establish practices ensuring the Army is complying with statutory norms for collection, maintenance, and dissemination of records. The Department of the Army received two comments from one commenter. No substantive changes were requested or made; however, the proposed changes were accepted and made to the final rule. The commenter expressed concern on § 505–2(e) titled ''Nomination of individuals when personal information * * *'' It was changed to read ''Notification of individuals when personal information * * *'' The other concern was in § 505.2(a)(2), suggestion was made to clarify the section by incorporating the DoD 6025.18–R, Privacy of Individually Identifiable Health Information in DoD Health Care Programs, language. The proposed § 505.2 (a)(3) through § 505.2(a)(13) was redesignated as § 505.2(a) (4) through § 505.2(a)(14) and a new § 505.2(a)(3) was added.

B. Executive Order 12866 (Regulatory Planning and Review)

It has been determined that Privacy Act rules for the Department of Defense are not significant rules. The rules do not (1) have an annual effect on the economy of $100 million or more or adversely affect in a material way the economy; a sector of the economy; productivity; competition; jobs; the environment; public health or safety; or State, local, or tribal governments or communities; (2) create a serious inconsistency or otherwise interfere with an action taken or planned by another Agency; (3) materially alter the budgetary impact of entitlements, grants, user fees, or loan programs, or the rights and obligations of recipients thereof; or (4) raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in this Executive order.

C. Regulatory Flexibility

It has been certified that Privacy Act rules for the Department of Defense do not have significant economic impact on a substantial number of small entities because they are concerned only with the administration of Privacy Act systems of records within the Department of Defense.

D. Paperwork Reduction Act

It has been certified that Privacy Act rules for the Department of Defense impose no information requirements beyond the Department of Defense and that the information collected within the Department of Defense is necessary and consistent with 5 U.S.C. 552a, known as the Privacy Act of 1974.

E. Unfunded Mandates Reform Act

It has been certified that the Privacy Act rulemaking for the Department of Defense does not involve a Federal mandate that may result in the expenditure by State, local and tribal governments, in the aggregate, or by the private sector, of $100 million or more and that such rulemaking will not significantly or uniquely affect small governments.

F. Executive Order 13132 (Federalism)

It has been certified that the Privacy Act rules for the Department of Defense do not have federalism implications. The rules do not have substantial direct effects on the States, on the relationship between the National Government and the States, or on the distribution of power and responsibilities among the various levels of government.

Robert Dickerson,

Chief, U.S. Army Freedom of Information Act and Privacy Office.

List of Subjects in 32 CFR Part 505

Privacy.

■ For reasons stated in the preamble the Department of the Army revises 32 CFR part 505 to read as follows:

PART 505—ARMY PRIVACY ACT PROGRAM

Sec.

Authority: Pub. L. 93–579, 88 Stat. 1896 (5 U.S.C. 552a).

§ 505.1 General information.

(a) *Purpose.* This part sets forth policies and procedures that govern personal information maintained by the Department of the Army (DA) in Privacy Act systems of records. This part also provides guidance on collecting and disseminating personal information in

general. The purpose of the Army Privacy Act 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 Federal agencies' collection, maintenance, use and disclosure of personal information about them. Additionally, this part promotes uniformity within the Army's Privacy Act Program.

(b) *References:* (1) Referenced publications are listed in Appendix A of this part.

(2) DOD Computer Matching Program and other Defense Privacy Guidelines may be accessed at the Defense Privacy Office Web site *http://www.defenselink.mil/privacy.*

(c) Definitions are provided at Appendix H of this part.

(d) *Responsibilities.* (1) The Office of the Administrative Assistant to the Secretary of the Army will—

(i) Act as the senior Army Privacy Official with overall responsibility for the execution of the Department of the Army Privacy Act Program;

(ii) Develop and issue policy guidance for the program in consultation with the Army General Counsel; and

(iii) Ensure the DA Privacy Act Program complies with Federal statutes, Executive Orders, Office of Management and Budget guidelines, and 32 CFR part 310.

(2) The Chief Attorney, Office of the Administrative Assistant to the Secretary of the Army (OAASA) will—

(i) Provide advice and assistance on legal matters arising out of, or incident to, the administration of the DA Privacy Act Program;

(ii) Serve as the legal advisor to the DA Privacy Act Review Board. This duty may be fulfilled by a designee in the Chief Attorney and Legal Services Directorate, OAASA;

(iii) Provide legal advice relating to interpretation and application of the Privacy Act of 1974; and

(iv) Serve as a member on the Defense Privacy Board Legal Committee. This duty may be fulfilled by a designee in the Chief Attorney and Legal Services Directorate, OAASA.

(3) The Judge Advocate General will serve as the Denial Authority on requests made pursuant to the Privacy Act of 1974 for access to or amendment of Army records, regardless of functional category, concerning actual or potential litigation in which the United States has an interest.

(4) The Chief, DA Freedom of Information Act and Privacy Office (FOIA/P), U.S. Army Records Management and Declassification Agency will—

(i) Develop and recommend policy;

(ii) Execute duties as the Army's Privacy Act Officer;

(iii) Promote Privacy Act awareness throughout the DA;

(iv) Serve as a voting member on the Defense Data Integrity Board and the Defense Privacy Board;

(v) Represent the Department of the Army in DOD policy meetings; and

(vi) Appoint a Privacy Act Manager who will—

(A) Administer procedures outlined in this part;

(B) Review and approve proposed new, altered, or amended Privacy Act systems of records notices and subsequently submit them to the Defense Privacy Office for coordination;

(C) Review Department of the Army Forms for compliance with the Privacy Act and this part;

(D) Ensure that reports required by the Privacy Act are provided upon request from the Defense Privacy Office;

(E) Review Computer Matching Agreements and recommend approval or denial to the Chief, DA FOIA/P Office;

(F) Provide Privacy Act training;

(G) Provide privacy guidance and assistance to DA activities and combatant commands where the Army is the Executive Agent;

(H) Ensure information collections are developed in compliance with the Privacy Act provisions;

(I) Ensure Office of Management and Budget reporting requirements, guidance, and policy are accomplished; and

(J) Immediately review privacy violations of personnel to locate the problem and develop a means to prevent recurrence of the problem.

(5) Heads of Department of the Army activities, field-operating agencies, direct reporting units, Major Army commands, subordinate commands down to the battalion level, and installations will—

(i) Supervise and execute the privacy program in functional areas and activities under their responsibility; and

(ii) Appoint a Privacy Act Official who will—

(A) Serve as the staff advisor on privacy matters;

(B) Ensure that Privacy Act records collected and maintained within the Command or agency are properly described in a Privacy Act system of records notice published in the **Federal Register**;

(C) Ensure no undeclared systems of records are being maintained;

(D) Ensure Privacy Act requests are processed promptly and responsively;

(E) Ensure a Privacy Act Statement is provided 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 personal information (i.e., forms, personal interviews, stylized formats, telephonic interviews, or other methods);

(F) Review, biennially, recordkeeping practices to ensure compliance with the Act, paying particular attention to the maintenance of automated records. In addition, ensure cooperation with records management officials on such matters as maintenance and disposal procedures, statutory requirements, forms, and reports; and

(G) Review, biennially Privacy Act training practices. This is to ensure all personnel are familiar with the requirements of the Act.

(6) DA Privacy Act System Managers and Developers will—

(i) Ensure that appropriate procedures and safeguards are developed, implemented, and maintained to protect an individual's personal information;

(ii) Ensure that all personnel are aware of their responsibilities for protecting personal information being collected and maintained under the Privacy Act Program;

(iii) Ensure official filing systems that retrieve records by name or other personal identifier and are maintained in a Privacy Act system of records have been published in the **Federal Register** as a Privacy Act system of records notice. Any official who willfully maintains a system of records without meeting the publication requirements, as prescribed by 5 U.S.C. 552a, as amended, OMB Circular A–130, 32 CFR part 310 and this part, will be subject to possible criminal penalties and/or administrative sanctions;

(iv) Prepare new, amended, or altered Privacy Act system of records notices and submit them to the DA Freedom of Information and Privacy Office for review. After appropriate coordination, the system of records notices will be submitted to the Defense Privacy Office for their review and coordination;

(v) Review, biennially, each Privacy Act system of records notice under their purview to ensure that it accurately describes the system of records;

(vi) Review, every four years, the routine use disclosures associated with each Privacy Act system of records notice in order to determine if such routine use continues to be compatible with the purpose for which the activity collected the information;

(vii) Review, every four years, each Privacy Act system of records notice for which the Secretary of the Army has

promulgated exemption rules pursuant to Sections (j) or (k) of the Act. This is to ensure such exemptions are still appropriate;

(viii) Review, every year, contracts that provide for the maintenance of a Privacy Act system of records to accomplish an activity's mission. This requirement is to ensure each contract contains provisions that bind the contractor, and its employees, to the requirements of 5 U.S.C. 552a(m)(1); and

(ix) 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. This additional review will ensure that the requirements of the Privacy Act, Office of Management and Budget guidance, local regulations, and the requirements contained in the Matching Agreements themselves have been met.

(7) All DA personnel will—

(i) Take appropriate actions to ensure personal information contained in a Privacy Act system of records is protected so that the security and confidentiality of the information is preserved;

(ii) Not disclose any personal information contained in a Privacy Act system of records except as authorized by 5 U.S.C. 552a, DOD 5400.11–R, or other applicable laws. Personnel willfully making a prohibited disclosure are subject to possible criminal penalties and/or administrative sanctions; and

(iii) Report any unauthorized disclosures or unauthorized maintenance of new Privacy Act systems of records to the applicable activity's Privacy Act Official.

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

(9) Commander, Army and Air Force Exchange Service, will supervise and execute the Privacy Program within that command pursuant to this part.

(10) Overall Government-wide responsibility for implementation of the Privacy Act is the Office of Management and Budget. The Department of Defense is responsible for implementation of the Act within the armed services. The Privacy Act also assigns specific Government-wide responsibilities to the Office of Personnel Management and the General Services Administration.

(11) Government-wide Privacy Act systems of records notices are available at *http://www.defenselink.mil/privacy.*

(e) *Legal Authority.* (1) Title 5, United States Code, Section 552a, as amended, The Privacy Act of 1974.

(2) Title 5, United States Code, Section 552, The Freedom of Information Act (FOIA).

(3) Office of Personnel Management, Federal Personnel Manual (5 CFR parts 293, 294, 297, and 7351).

(4) OMB Circular No. A–130, Management of Federal Information Resources, Revised, August 2003.

(5) DOD Directive 5400.11, Department of Defense Privacy Program, November 16, 2004.

(6) DOD Regulation 5400.11–R, Department of Defense Privacy Program, August 1983.

(7) Title 10, United States Code, Section 3013, Secretary of the Army.

(8) Executive Order No. 9397, Numbering System for Federal Accounts Relating to Individual Persons, November 30, 1943.

(9) Public Law 100–503, the Computer Matching and Privacy Act of 1974.

(10) Public Law 107–347, Section 208, Electronic Government (E-Gov) Act of 2002.

(11) DOD Regulation 6025.18–R, DOD Health Information Privacy Regulation, January 24, 2003.

§ 505.2 General 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 United States living citizens and aliens lawfully admitted for permanent residence from unwarranted intrusion.

(2) Deceased individuals do not have Privacy Act rights, nor do executors or next-of-kin in general. However, immediate family members may have limited privacy rights in the manner of death details and funeral arrangements of the deceased individual. Family members often use the deceased individual's Social Security Number (SSN) for federal entitlements; appropriate safeguards must be implemented to protect the deceased individual's SSN from release. Also, the Health Insurance Portability and Accountability Act extends protection to certain medical information contained in a deceased individual's medical records.

(3) Personally identifiable health information of individuals, both living and deceased, shall not be used or disclosed except for specifically permitted purposes.

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

(5) Maintain only personal information that 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 an approved National Archives and Records Administration record disposition.

(8) Let individuals know what Privacy Act records the Army maintains by publishing Privacy Act system of records notices in the **Federal Register**. This will enable individuals to review and make copies of these records, subject to the exemptions authorized by law and approved by the Secretary of the Army. Department of the Army Privacy Act systems of records notices are available at *http://www.defenselink.mil/privacy.*

(9) Permit individuals to correct and amend records about themselves which they can prove are factually in error, not timely, not complete, not accurate, or not relevant.

(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) Maintain no 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 assemblage, 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.

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

(2) Personal information should never be placed on shared drives that are accessed by groups of individuals unless each person has an ''official need to know'' the information in 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 380–67, The Department of the Army Personnel Security Program.

(c) *Conveying privacy protected data electronically via e-mail and the World Wide Web.* (1) Unencrypted electronic transmission of privacy protected data makes the Army vulnerable to information interception which can cause serious harm to the individual and the accomplishment of the Army's mission.

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

(3) Privacy Web sites and hosted systems with privacy-protected data will employ secure sockets layers (SSL) and Public Key Infrastructure (PKI) encryption certificates or other DoD-approved commercially available certificates for server authentication and client/server authentication. Individuals who transmit data containing personally identifiable information over e-mail will employ PKI or other DoD-approved certificates.

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

(i) There is an ''official need to know'' for each addressee (including ''cc'' addressees); and

(ii) The Privacy Act protected information 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 e-mail message, along with the following language: ''This contains FOR OFFICIAL USE ONLY (FOUO) information which is protected under the Privacy Act of 1974 and AR 340–21, The Army Privacy Program. Do not further disseminate this information without the permission of the sender.''

(iii) Do not indiscriminately apply this statement. Use it only in situations when actually transmitting protected Privacy Act information.

(iv) For additional information about marking documents ''FOUO'' review AR 25–55, Chapter IV.

(5) Add appropriate ''Privacy and Security Notices'' at major Web site entry points. Refer to AR 25–1, para 6–4n for requirements for 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.defenselink.mil/webmasters/policy/DOD_web_policy.*

(6) Ensure public Web sites comply with policies regarding restrictions on persistent and third party cookies. The Army prohibits both persistent and third part cookies. (see AR 25–1, para 6–4n)

(7) A Privacy Advisory is required on Web sites which host information systems soliciting personally identifying information, even when not maintained in a Privacy Act system of records. The Privacy Advisory informs the individual why the information is solicited and how it will be used. Post the Privacy Advisory to the Web site page where the information is being solicited, or to a well marked hyperlink stating ''Privacy Advisory—Please refer to the Privacy and Security Notice that describes why this information is collected and how it will be used.''

(d) *Protecting records containing personal identifiers such as names and Social Security Numbers.* (1) Only those records covered by a Privacy Act system of records notice may be arranged to permit retrieval by a personal identifier (e.g., an individual's name or Social Security Number). AR 25–400–2, paragraph 6–2 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.

(2) Use a coversheet or DA Label 87 (For Official Use Only) for individual records not contained in properly labeled file folders or cabinets.

(3) When developing a coversheet, the following is an example of a statement that you may use: ''The information contained within is FOR OFFICIAL USE ONLY (FOUO) and protected by the Privacy Act of 1974.''

(e) *Notification of Individuals when personal information is lost, stolen, or compromised.* (1) Whenever an Army organization becomes aware the protected personal information pertaining to a Service member, civilian employee (appropriated or non-appropriated fund), military retiree, family member, or another individual affiliated with Army organization (e.g., volunteer) has been lost, stolen, or compromised, the organization shall inform the affected individuals as soon as possible, but not later than ten days after the loss or compromise of protected personal information is discovered.

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

(3) 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 of the Secretary of the Army to explain why the affected individuals or population's personal information has been lost, stolen, or compromised.

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

(f) *Federal government contractors' compliance.* (1) When a DA activity contracts for the design, development, or operation of a Privacy Act system of records in order to accomplish a DA mission, the agency must apply the requirements of the Privacy Act to the contractor and its employees working on the contract (See 48 CFR part 24 and other applicable supplements to the FAR; 32 CFR part 310).

(2) System Managers will review annually, contracts contained within the system(s) of records under their responsibility, to determine which ones contain provisions relating to the design, development, or operation of a Privacy Act system of records.

(3) Contractors are considered employees of the Army for the purpose of the sanction provisions of the Privacy Act during the performance of the contract requirements.

(4) Disclosing records to a contractor for use in performing the requirements of an authorized DA contract is considered a disclosure within the agency under exception (b)(1), ''Official Need to Know'', of the Act.

§ 505.3 Privacy Act systems of records.

(a) *Systems of records.* (1) A system of records is a group of records under the control of a DA activity that are retrieved by an individual's name or by some identifying number, symbol, or other identifying particular assigned to an individual.

(2) Privacy Act systems of records must be—

(i) Authorized by Federal statute or an Executive Order;

(ii) Needed to carry out DA's mission; and

(iii) Published in the **Federal Register** in a system of records notice, which will provide the public an opportunity to

comment before DA implements or changes the system.

(3) The mere fact that records are retrievable by a name or personal identifier is not enough. Records must actually be retrieved by a name or personal identifier. Records in a group of records that may be retrieved by a name or personal identifier but are not normally retrieved by this method are not covered by this part. However, they are covered by AR 25–55, the Department of the Army Freedom of Information Act Program.

(4) The existence of a statute or Executive Order mandating the maintenance of a system of records to perform an authorized activity does not abolish the responsibility to ensure the information in the system of records is relevant and necessary to perform the authorized activity.

(b) *Privacy Act system of records notices.* (1) DA must publish notices in the **Federal Register** on new, amended, altered, or deleted systems of records to inform the public of the Privacy Act systems of records that it maintains. The Privacy Act requires submission of new or significantly changed systems of records to OMB and both houses of Congress before publication in the **Federal Register** (See Appendix E of this part).

(2) Systems managers must send a proposed notice at least 120 days before implementing a new, amended or altered system to the DA Freedom of Information and Privacy Office. The proposed or altered notice must include a narrative statement and supporting documentation. A narrative statement must contain the following items:

(i) System identifier and name;

(ii) Responsible Official, title, and phone number;

(iii) If a new system, the purpose of establishing the system or if an altered system, nature of changes proposed;

(iv) Authority for maintenance of the system;

(v) Probable or potential effects of the system on the privacy of individuals;

(vi) Whether the system is being maintained, in whole or in part, by a contractor;

(vii) Steps taken to minimize risk of unauthorized access;

(viii) Routine use compatibility;

(ix) Office of Management and Budget information collection requirements; and

(x) Supporting documentation as an attachment. Also as an attachment should be the proposed new or altered system notice for publication in the **Federal Register**.

(3) An amended or altered system of records is one that has one or more of the following:

(i) A significant increase in the number, type, or category of individuals about whom records are maintained;

(ii) A change that expands the types of categories of information maintained;

(iii) A change that alters the purpose for which the information is used;

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

(v) An addition of an exemption pursuant to Section (j) or (k) of the Act; or

(vi) An addition of a routine use pursuant to 5 U.S.C. 552a(b)(3).

(4) For additional guidance contact the DA FOIA/P Office.

(5) On behalf of DA, the Defense Privacy Office maintains a list of DOD Components' Privacy Act system of records notices at the Defense Privacy Office's Web site *http://www.defenselink.mil/privacy.*

(6) DA PAM 25–51 sets forth procedures pertaining to Privacy Act system of records notices.

(7) For new systems, system managers must establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records. This applies to all new systems of records whether maintained manually or automated.

(i) One safeguard plan is the development and use of a Privacy Impact Assessment (PIA) mandated by the E-Gov Act of 2002, Section 208. The Office of Management and Budget specifically directs that a PIA be conducted, reviewed, and published for all new or significantly altered information in identifiable form collected from or about the members of the public. The PIA describes the appropriate administrative, technical, and physical safeguards for new automated systems. This will assist in the protection against any anticipated threats or hazards to the security or integrity of data, which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. Contact your local Information Officer for guidance on conducting a PIA.

(ii) The development of appropriate safeguards must be tailored to the requirements of the system as well as other factors, such as the system environment, location, and accessibility.

§ 505.4 Collecting personal information.

(a) *General provisions.* (1) Employees will collect personal information to the greatest extent practicable directly from the subject of the record. This is especially critical, if the information may result in adverse determinations about an individual's rights, benefits, and privileges under federal programs (*See* 5 U.S.C. 552a(e)(2)).

(2) 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. Executive Order 9397 does not mandate the solicitation of SSNs from Army personnel as a means of identification.

(3) 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 Privacy Act Statement 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.

(4) When asking an individual for his or her SSN or other personal information that will be maintained in a system of records, the individual must be provided with a Privacy Act Statement.

(b) *Privacy Act Statement (PAS).* (1) A Privacy Act Statement is required whenever personal information is requested from an individual and will become part of a Privacy Act system of records. The information will be retrieved by the individual's name or other personal identifier (*See* 5 U.S.C. 552a(e)(3)).

(2) The PAS will ensure that individuals know why the information is being collected so they can make an

informed decision as to providing the personal information.

(3) In addition, the PAS will include language that is explicit, easily understood, and not so lengthy as to deter an individual from reading it.

(4) A sign can be displayed in areas where people routinely furnish this kind of information, and a copy of the PAS will be made available upon request by the individual.

(5) Do not ask the person to sign the PAS.

(6) A Privacy Act Statement must include the following four items—

(i) *Authority:* Cite the specific statute or Executive Order, including a brief title or subject that authorizes the DA to collect the personal information requested.

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

(iii) *Routine Uses:* A list of where and why the information will be disclosed OUTSIDE of DOD. Applicable routine uses are published in the applicable Privacy Act system of records notice(s). If none, the language to be used is: ''Routine Use(s): None. However the 'Blanket Routine Uses' set forth at the beginning of the Army's compilation of systems of records notices apply.''

(iv) *Disclosure:* Voluntary or Mandatory. Include in the Privacy Act Statement specifically whether furnishing the requested personal data is mandatory or voluntary. A requirement to furnish personal data 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 receiving the benefit or privilege, providing the information is always 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.

(7) Some acceptable means of administering the PAS are as follows, in the order of preference—

(i) Below the title of the media used to collect the personal information. The PAS should be positioned so that the individual will be advised of the PAS before he or she provides the requested information;

(ii) Within the body with a notation of its location below the title;

(iii) On the reverse side with a notation of its location below the title;

(iv) Attached as a tear-off sheet; or

(v) Issued as a separate supplement.

(8) An example of a PAS is at appendix B of this part.

(9) Include a PAS on a Web site page if it collects information directly from an individual and is retrieved by his or her name or personal identifier (See Office of Management and Budget Privacy Act Guidelines, 40 FR 28949, 28961 (July 9, 1975)).

(10) Army policy prohibits the collection of personally identifying information on public Web sites without the express permission of the user. Requests for exceptions must be forwarded to the Army CIO/G–6. (See AR 25–1, para 6–4n.)

(c) *Collecting personal information from third parties.* (1) It may not be practical to collect personal information directly from the individual in all cases. Some examples of when collection from third parties may be necessary are when—

(i) Verifying information;

(ii) Opinions or evaluations are needed;

(iii) The subject cannot be contacted; or

(iv) At the request of the subject individual.

(2) When asking third parties to provide information about other individuals, they will be advised of—

(i) The purpose of the request; and

(ii) Their rights to confidentiality as defined by the Privacy Act of 1974 (Consult with your servicing Staff Judge Advocate for potential limitations to the confidentiality that may be offered pursuant to the Privacy Act).

(d) *Confidentiality promises.* Promises of confidentiality must be prominently annotated in the record to protect from disclosure any information provided in confidence pursuant to 5 U.S.C. 552a(k)(2), (k)(5), or (k)(7).

§ 505.5 Individual access to personal information.

(a) *Individual access.* (1) The access provisions of this part are intended for use by individuals whose records are maintained in a Privacy Act system of records. If a representative acts on their behalf, a written authorization must be provided, with the exception of members of Congress acting on behalf of a constituent.

(2) A Department of the Army ''Blanket Routine Use'' allows the release of Privacy Act protected information to members of Congress when they are acting on behalf of the constituent and the information is filed and retrieved by the constituent's name or personal identifier. The said ''Blanket Routine Use'' is listed below.

''Congressional Inquiries Disclosure Routine Use: Disclosure from a system of records maintained by a DOD Component 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.''

(3) 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, unless—

(i) The information is subject to an exemption, the system manager has invoked the exemption, and the exemption is published in the **Federal Register**; or

(ii) The information was compiled in reasonable anticipation of a civil action or proceeding.

(4) Legal guardians or parents acting on behalf of a minor child have the minor child's rights of access under this part, unless the records were created or maintained pursuant to circumstances where the interests of the minor child were adverse to the interests of the legal guardian or parent.

(5) These provisions should allow for the maximum release of information consistent with Army and DOD's statutory responsibilities.

(b) *Individual requests for access.* (1) Individuals will address 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 systems of records notices (See DA PAM 25–51 or the Defense Privacy Office's Web site *http://www.defenselink.mil/privacy*).

(2) Individuals do not have to state a reason or justify the need to gain access to records under the Act.

(3) Release of personal information to individuals under this section is not considered a ''public release'' of information.

(c) *Verification of identity for first party requesters.* (1) Before granting access to personal data, an individual will provide reasonable verification of identity.

(2) When requesting records in writing, the preferred method of verifying identity is the submission of a notarized signature. An alternative method of verifying identity for individuals who do not have access to notary services is the submission of an un-sworn declaration in accordance with 28 U.S.C. 1746 in the following format:

(i) If executed within the United States, its territories, possessions, or commonwealths: ''I declare (or certify,

verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)''.

(ii) 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).''

(3) When an individual seeks access in person, identification can be verified by documents normally carried by the individual (such as identification card, driver's license, or other license, permit or pass normally used for identification purposes). However, level of proof of identity is commensurate with the sensitivity of the records sought. For example, more proof is required to access medical records than is required to access parking records.

(4) Telephonic requests will not be honored.

(5) An individual cannot be denied access solely for refusal to provide his or her Social Security Number (SSN) unless the SSN was required for access by statute or regulation adopted prior to January 1, 1975.

(6) If an individual wishes to have his or her records released directly to a third party or to be accompanied by a third party when seeking access to his or her records, reasonable proof of authorization must be obtained. The individual may be required to furnish a signed access authorization with a notarized signature or other proof of authenticity (*i.e.* telephonic confirmation) before granting the third party access.

(d) *Individual access to medical records.* (1) An individual must be given access to his or her medical and psychological records unless a judgment is made that access to such records could have an adverse effect on the mental or physical health of the individual. This determination normally should be made in consultation with a medical doctor. Additional guidance is provided in DOD 5400.11–R, Department of Defense Privacy Program. In this instance, the individual will be asked to provide the name of a personal health care provider, and the records will be provided to that health care provider, along with an explanation of why access without medical supervision could be harmful to the individual.

(2) Information that may be harmful to the record subject should not be released to a designated individual unless the designee is qualified to make psychiatric or medical determinations.

(3) DA activities may offer the services of a military physician, other than the one who provided the treatment.

(4) Do not require the named health care provider to request the records for the individual.

(5) The agency's decision to furnish the records to a medical designee and not directly to the individual is not considered a denial for reporting purposes under the Act and cannot be appealed.

(6) However, no matter what the special procedures are, DA has a statutory obligation to ensure that access is provided the individual.

(7) Regardless of age, all DA military personnel and all married persons are considered adults. The parents of these individuals do not have access to their medical records without written consent of the individual.

(8) DOD 6025.18–R, DOD Health Information Privacy Regulation, issued pursuant to the Health Insurance Portability and Accountability Act (HIPAA) of 1996, has placed additional procedural requirements on the uses and disclosure of individually identifiable health information beyond those found in the Privacy Act of 1974 and this part. In order to be in compliance with HIPAA, the additional guidelines and procedures will be reviewed before release of an individual's identifiable health information.

(e) *Personal notes.* (1) The Privacy Act does not apply to personal notes of individuals used as memory aids. These documents are not Privacy Act records and are not subject to this part.

(2) The five conditions for documents to be considered personal notes are as follows—

(i) Maintained and discarded solely at the discretion of the author;

(ii) Created only for the author's personal convenience and the notes are restricted to that of memory aids;

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

(iv) Not shown to others for any reason; and

(v) Not filed in agency files.

(3) Any disclosure from personal notes, either intentional or through carelessness, removes the information from the category of memory aids and the personal notes then become subject to provisions of the Act.

(f) *Denial or limitation of individual's right to access.* (1) Even if the information is filed and retrieved by an individual's name or personal identifier, his or her right to access may be denied if—

(i) The records were compiled in reasonable anticipation of a civil action or proceeding including any action where DA expects judicial or administrative adjudicatory proceedings. The term ''civil action or proceeding'' includes quasi-judicial, pre-trial judicial, and administrative proceedings, as well as formal litigation;

(ii) The information is about a third party and does not pertain to the requester. A third party's SSN and home address will be withheld. However, information about the relationship between the individual and the third party would normally be disclosed as it pertains to the individual;

(iii) The records are in a system of records that has been properly exempted by the Secretary of the Army from the access provisions of this part and the information is exempt from release under a provision of the Freedom of Information Act (See appendix C of this part for a list of applicable Privacy Act exemptions, exceptions, and ''Blanket'' routine uses);

(iv) The records contain properly classified information that has been exempted from the access provision of this part;

(v) The records are not described well enough to enable them to be located with a reasonable amount of effort on the part of an employee familiar with the file. Requesters should reasonably describe the records they are requesting. They do not have to designate a Privacy Act system of records notice identification number, but they should at least identify a type of record or functional area. For requests that ask for ''all records about me,'' DA personnel should ask the requester for more information to narrow the scope of his or her request; and

(vi) Access is sought by an individual who fails or refuses to comply with Privacy Act established procedural requirements, included refusing to pay fees.

(2) Requesters will not use government equipment, supplies, stationery, postage, telephones, or official mail channels for making Privacy Act requests. System managers will process such requests but inform requesters that using government resources to make Privacy Act requests is not authorized.

(3) When a request for information contained in a Privacy Act system of records is denied in whole or in part, the Denial Authority or designee shall inform the requester in writing and explain why the request for access has been refused.

(4) A request for access, notification, or amendment of a record shall be acknowledged in writing within 10 working days of receipt by the proper system manager or record custodian.

(g) *Relationship between the Privacy Act and the Freedom of Information Act.* (1) Not all requesters are knowledgeable of the appropriate statutory authority to cite when requesting information. In some instances, they may cite neither the PA nor the Freedom of Information Act in their request. In some instances they may cite one Act but not the other. The Freedom of Information Act and the PA works together to ensure that requesters receive the greatest amount of information possible.

(2) Do not deny the individual access to his or her records simply because he or she failed to cite the appropriate statute or regulation.

(3) If the records are required to be released under the Freedom of Information Act, the PA will never block disclosure to requester. If the PA allows the DA activity to deny access to an individual, the Freedom of Information Act must still be applied, and the information released if required by the Freedom of Information Act.

(4) Unlike the Freedom of Information Act, the Privacy Act applies only to U.S. citizens and aliens lawfully admitted for permanent residence.

(5) Requesters who seek records about themselves contained in a Privacy Act system of records (1st party requesters) and who cite or imply only the Privacy Act, will have their request processed under the provisions of both the PA and the Freedom of Information Act. If the information requested is not contained in a Privacy Act system of records or is not about the requester, the individual's request will be processed under the provisions of the Freedom of Information Act only, and the Freedom of Information Act processing requirements/time lines will apply.

(6) *Third party information.* (i) Third party information contained in a Privacy Act system of records that does not pertain to the requester, such as SSN, home addresses, and other purely personal information that is not about the requester, will be processed under the provisions of Freedom of Information Act only. Third party information that is not about the requester is not subject to the Privacy Act's first party access provision.

(ii) Information about the relationship between the first party requester and a third party is normally disclosed as pertaining to the first party requester. Consult your servicing Staff Judge Advocate if there is a question about the release of third party information to a first party requester.

(7) If an individual requests information about them contained in a Privacy Act system of records, the individual may be denied the information only if the information is exempt under both the PA and the Freedom of Information Act. Both PA and Freedom of Information Act exemptions will be cited in the denial letter and appeals will be processed in accordance with both Acts.

(8) Each time a first party requester cites or implies the PA, perform this analysis:

(i) Is the request from a United States living citizen or an alien lawfully admitted for permanent residence?

(ii) Is the individual requesting an agency record?

(iii) Are the records within a PA system of records that are filed and retrieved by an individual's name or other personal identifier? (If the answer is ''yes'' to all of these questions, then the records should be processed under the ''Privacy Act'') and

(iv) Does the information requested pertain exclusively to the requester?

(A) If yes, no further consideration of Freedom of Information Act exemptions required. Release all information unless a PA exemption authorizes withholding.

(B) If no, process the information that is not about the requester under the Freedom of Information Act and withhold only if a proper Freedom of Information Act exemption applies.

(h) *Functional requests.* If an individual asks for his or her records and does not cite or reasonably imply either the Privacy Act or the Freedom of Information Act, and another prescribing directive or regulation authorizes the release, the records should be released under that other directive or regulation and not the PA or the FOIA. Examples of functional requests are military members asking to see their Official Military Personnel Records or civilian employees asking to see their Official Personnel Folder.

(i) *Procedures for denying or limiting an individual's right to access or amendment and the role of the Denial Authority.* (1) The only officials authorized to deny a request for records or a request to amend records in a PA system of records pertaining to the requesting individual, are the appropriate Denial Authorities, their designees, or the Secretary of the Army who will be acting through the General Counsel.

(2) Denial Authorities are authorized to deny requests, either in whole or in part, for notification, access and amendment of Privacy Act records contained in their respective areas of responsibility.

(i) The Denial Authority may delegate all or part of their authority to a division chief under his supervision within the Agency in the grade of 0–5/GS–14 or higher. All delegations must be in writing.

(ii) The Denial Authority will send the names, office names, and telephones numbers of their delegates to the DA Freedom of Information and Privacy Office.

(iii) 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.

(iv) The official Denial Authorities are for records under their authority (See appendix B of this part). The individuals designated as Denial Authorities under this part are the same individuals designated as Initial Denial Authorities under AR 25–55, the Department of the Army Freedom of Information Act Program. However, delegation of Denial Authority pursuant to this part does not automatically encompass delegation of Initial Denial Authority under AR 25–55. Initial Denial Authority must be expressly delegated pursuant to AR 25–55 for an individual to take action on behalf of an Initial Denial Authority under AR 25–55.

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

(4) Requests for information recommended for denial will be forwarded to the appropriate Denial Authority, along with a copy of the records and justification for withholding the record. At the same time, notify the requester of the referral to the Denial Authority for action. All documents or portions thereof determined to be releasable to the requester will be released to the requester before forwarding the case to the Denial Authority.

(5) 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.

(6) Included in the notification will be:

(i) Denying Official's name, position title, and business address;

(ii) Date of the denial;

(iii) The specific reason for the denial, citing the appropriate subsections of the Privacy Act, the Freedom of Information Act, AR 25–55, The Department of the Army Freedom of Information Act Program and this part; and

(iv) 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.

(7) The appeal must be in writing and the requester should provide a copy of the denial letter and a statement of their reasons for seeking review.

(8) 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 Defense Privacy Office's Web site *http://www.defenselink.mil/privacy* or DA PAM 25–51.

(j) *No records determinations.* (1) Since a no record response may be considered an ''adverse'' determination, the Denial Authority must make the final determination that no records exist. The originating agency shall notify the requester that an initial determination has been made that there are no responsive records, however the final determination will be made by the Denial Authority. A no records certificate must accompany a no records determination that is forwarded to the Denial Authority.

(2) The Denial Authority must provide the requester with appeal rights.

(k) *Referral of requests.* (1) A request received by a DA activity having no records responsive to a request shall be referred to another DOD Component or DA activity, if the other Component or activity confirms that they have the requested records, or verifies that they are the proper custodian for that type of record. The requester will be notified of the referral. In cases where the DA activity receiving the request has reason to believe that the existence or nonexistence of the record may in itself be classified, that activity will consult the Component or activity having cognizance over the records in question before referring the request. If the Component or activity that is consulted determines that the existence or nonexistence of the records is in itself classified, the requester shall be so notified by the DA activity originally receiving the request that it can neither confirm nor deny the existence of the record, and no referral shall take place.

(2) A DA activity shall refer a Privacy Act request for a classified record that it holds to another DOD Component, DA activity, or agency outside the Department of Defense, if the record originated in the other DOD Component, DA activity, or outside agency, or if the classification is derivative. The referring DA activity will provide the records and a release recommendation with the referral action.

(3) Any DA activity receiving a request that has been misaddressed will refer the request to the proper address and advise the requester.

(4) Within DA, referrals will be made directly to offices having custody of the requested records (unless the Denial Authority is the custodian of the requested records). If the office receiving the Privacy Act request does not know where the requested records are located, the office will contact the DA FOIA/P Office, to determine the appropriate office for referral.

(5) The requester will be informed of the referral whenever records or a portion of records are, after prior consultation, referred to another activity for a release determination and direct response. Additionally, the DA activity referral letter will accomplish the following—

(i) Fully describe the Privacy Act system of records from which the document was retrieved; and

(ii) Indicate whether the referring activity claims any exemptions in the Privacy Act system of records notice.

(6) Within the DA, an activity will refer a Privacy Act request for records that it holds but was originated by another activity, to the originating activity for direct response. An activity will not, in any case, release or deny such records without prior consultation with the originating activity. The requester will be notified of such referral.

(7) A DA activity may refer a Privacy Act request for records that originated in an agency outside of DOD, or that is based on information obtained from an agency outside the DOD, to that agency for direct response to the requester, only if that agency is subject to the Privacy Act. Otherwise, the DA activity must respond to the request.

(8) DA activities will not honor any Privacy Act requests for investigative, intelligence, or any other type of records that are on loan to the Department of Defense for a specific purpose, if the records are restricted from further release in writing. Such requests will be referred to the agency that provided the records.

(9) A DA activity will notify requesters seeking National Security Council (NSC) or White House documents that they should write directly to the NSC or White House for such documents. DA documents in which the NSC or White House have a concurrent reviewing interest will be forwarded to the Department of Defense, Office of Freedom of Information and Security Review, which will coordinate with the NSC or White House, and return the documents to the originating DA activity after NSC or White House review. NSC or White House documents discovered in DA activity files which are responsive to a Privacy Act request will be forwarded to DOD for coordination and return with a release determination.

(10) To the extent referrals are consistent with the policies expressed above; referrals between offices of the same DA activity are authorized.

(l) *Reproduction fees.* (1) Use fees only to recoup direct reproduction costs associated with granting access.

(2) DA activities may use discretion in their decision to charge for the first copy of records provided to an individual to whom the records pertain. Thereafter, fees will be computed pursuant to the fee schedule set forth in AR 25–55, including the fee waiver provisions.

(3) Checks or money orders for fees should be made payable to the Treasurer of the United States and will be deposited in the miscellaneous receipts of the treasury account maintained at the activity's finance office.

(4) Reproduction costs shall only include the direct costs of reproduction and shall not include costs of—

(i) Time or effort devoted to searching for or reviewing the records by personnel;

(ii) Fees not associated with the actual cost of reproduction;

(iii) Producing a copy when it must be provided to the individual without cost under another regulation, directive, or law;

(iv) Normal postage;

(v) Transportation of records or personnel; or

(vi) Producing a copy when the individual has requested only to review the records and has not requested a copy, and the only means of allowing review is to make a copy (e.g., the records are stored in a computer and a copy must be printed to provide individual access, or the activity does not wish to surrender temporarily the original records for the individual to review).

(m) *Privacy Act case files.* (1) Whenever an individual submits a Privacy Act request, a case file will be established. This Privacy Act case file is a specific type of file that is governed by a specific Privacy Act system of records notice. In no instance will the individual's Privacy Act request and

corresponding Army actions be included in the individual's military personnel file or other military filing systems, such as adverse action files or general legal files, and in no instance will the Privacy Act case file be used to make an adverse determination about the individual.

(2) The case file will be comprised of the request for access/amendment, grants, refusals, coordination action(s), and all related papers.

§ 505.6 Amendment of records.

(a) *Amended records.* (1) 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 part.

(2) 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.

(3) The system manager or custodian must review Privacy Act records for accuracy, relevance, timeliness, and completeness.

(4) 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 (*e.g.*, 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/proceedings.

(b) *Proper amendment requests.* (1) Amendment requests, except for routine administrative changes, will be in writing.

(2) When acting on behalf of a first party requester, an individual must provide written documentation of the first party requester's consent to allow the individual to view his or her records.

(3) Amendment is appropriate if it can be shown that—

(i) Circumstances leading up to the recorded event were found to be inaccurately reflected in the document;

(ii) The record is not identical to the individual's copy; or

(iii) The document was not constructed in accordance with the applicable recordkeeping requirements prescribed in AR 25–400–2, The Army Records Information Management System (ARIMS).

(4) Under the amendment provisions, an individual may not challenge the merits of an adverse determination.

(5) U.S. Army Criminal Investigation Command (USACIDC) reports of investigations (PA system of records notice A0195–2a USACIDC, Source Register; A0195–2b USACIDC, Criminal Investigation and Crime Laboratory Files) have been exempted from the amendment provisions of the Privacy Act. Requests to amend these reports will be considered under AR 195–2. Actions taken 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.

(6) 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.

(7) 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.

(8) Other records that are exempt from the amendment provisions of the Privacy Act are listed in the applicable PA system of records notices.

(c) *Amendment procedures.* (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 (e.g., deletion, addition, or amendment). The burden of proof is on the requester. 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.

(2) Records for which amendment is sought must be reviewed by the proper system manager or custodian for accuracy, relevance, timeliness, and completeness.

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

(4) 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.

(5) 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.

(6) 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.

(i) On receipt of a request for further review by the Privacy Act Review Board, the Denial Authority will append any additional records or background information that substantiates the refusal or renders the case complete;

(ii) Within 5 working days of receipt, forward the appeal to the DA Privacy Act Review Board; and

(iii) Append the servicing Judge Advocate's legal review, including a determination that the Privacy Act Review Board packet is complete.

(d) *DA Privacy Act Review Board.* (1) 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.

(2) 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.

(3) The Board membership consists of the following principal members, comprised of three voting and two non-voting members, or their delegates.

(4) Three voting members include—

(i) Administrative Assistant to the Secretary of the Army (AASA) who acts as the Chairman of the Board;

(ii) The Judge Advocate General; and

(iii) The Chief, DA Freedom of Information and Privacy Division, U.S. Army Records Management and Declassification Agency.

(5) In addition, two non-voting members include—

(i) The Chief Attorney, OAASA (or designee) who serves as the legal advisor and will be present at all Board sessions to provide legal advice as required; and

(ii) Recording Secretary provided by the Office of the Administrative Assistant to the Secretary of the Army.

(e) *DA Privacy Act Review Board meetings.* (1) The meeting of the Board requires the presence of all five members or their designated representatives. Other non-voting members with subject matter expertise may participate in a meeting of the Board, at the discretion of the Chairman.

(2) Majority vote of the voting members is required to make a final determination on a request before the Board.

(3) Board members, who have denial authority, may not vote on a matter upon which they took Denial Authority action. However, an individual who took Denial Authority action, or his or her representative, may serve as a non-voting member when the Board considers matters in the Denial Authority's area of functional specialization.

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

(5) If the Board determines that an amendment is warranted (the record is inaccurate as a matter of fact rather than judgment, irrelevant, untimely, or incomplete) it 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.

(6) If the Board determines that amendment is unwarranted, they will—

(i) Obtain the General Counsel's concurrence in writing;

(ii) Respond to the requester with the reasons for denial; and

(iii) 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 was disputed. The disclosing authority may include a brief summary of the Board's reasons for not amending the disputed record.

(7) It is inappropriate for the Privacy Act Review Board to consider any record which is exempt from the amendment provision of the Privacy Act.

§ 505.7 Disclosure of personal information to other agencies and third parties.

(a) *Disclosing records to third parties.* (1) DA is prohibited from disclosing a record from a Privacy Act system of records to any person or agency without the prior written consent of the subject of the record, except when—

(i) Pursuant to the twelve Privacy Act exceptions. The twelve exceptions to the ''no disclosure without consent'' rule are those exceptions which permit the release of personal information without the individual's/subject's consent (See appendix C of this part).

(ii) The FOIA requires the release of the record. One of the twelve exceptions to Privacy Act is the FOIA Exception. If the FOIA requires the release of information, the information must be released. The Privacy Act can not prevent release to a third party if the FOIA requires release. However, information must not be discretionarily released under the FOIA if the information is subject to the Privacy Act's ''no disclosure without consent'' rule.

(iii) A routine use applies. Another major exception to the ''no disclosure without consent'' rule is the routine use exception. The Privacy Act allows federal agencies to publish routine use exceptions to the Privacy Act. Some routine uses are Army specific, DOD specific, and Governmentwide. Routine uses exceptions are listed in the Privacy Act system of records notice(s) applicable to the Privacy Act records in question. The Army and other agencies' system of records notices may be accessed at the Defense Privacy Office's Web site *http://www.defenselink.mil/privacy.*

(2) The approved twelve exceptions to the Privacy Act ''no disclosure without consent'' rule are listed at appendix C of this part.

(b) *Disclosing records to other DOD components and to federal agencies outside the DOD.* (1) The twelve Privacy Act exceptions referred to in appendix C of this part are available to other DOD components and to federal agencies outside the DOD as exceptions to the Privacy Act's ''no disclosure without consent'' rule, with the exception of the FOIA exception. The FOIA is not an appropriate mechanism for providing information to other DOD components and to federal agencies outside the DOD.

(2) A widely used exception to requests for information from local and state government agencies and federal agencies not within the DOD is the routine use exception to the Privacy Act.

(3) The most widely used exception to requests for information from other DOD components is the ''intra-agency need to know'' exception to the Privacy Act. Officers and employees of the DOD who have an official need for the records in the performance of their official duties are entitled to Privacy Act protected information. Rank, position, or title alone does not authorize access to personal information about others. An official need for the information must exist before disclosure.

(4) For the purposes of disclosure and disclosure accounting, the Department of Defense (DOD) is considered a single agency.

(c) *Disclosures under AR 25–55, the Freedom of Information Act (FOIA) Program.* (1) Despite Privacy Act protections, all records must be disclosed if the Freedom of Information Act (FOIA) requires their release. The FOIA requires release unless the information is exempted by one or more of the nine FOIA exemptions.

(2) Required release under the FOIA. The following are examples of personal information that is generally not exempt from the FOIA; therefore, it must be released to the public, unless covered by paragraphs (d)(2) and (d)(3) of this section. The following list is not all inclusive:

(i) Military Personnel—

(A) Rank, date of rank, active duty entry date, basic pay entry date, and gross pay (including base pay, special pay, and all allowances except Basic Allowance for Housing);

(B) Present and past duty assignments, future stateside assignments;

(C) Office/unit name, duties address and telephone number (DOD policy may require withholding of this information in certain circumstances);

(D) Source of commission, promotion sequence number, military awards and decorations, and professional military education;

(E) Duty status, at any given time;

(F) Separation or retirement dates;

(G) Military occupational specialty (MOS);

(H) Active duty official attendance at technical, scientific or professional meetings; and

(I) Biographies and photos of key personnel (DOD policy may require withholding of this information in certain circumstances).

(ii) Federal civilian employees—

(A) Present and past position titles, occupational series, and grade;

(B) Present and past annual salary rates (including performance awards or bonuses, incentive awards, merit pay amount, Meritorious or Distinguished Executive Ranks, and allowances and differentials);

(C) Present and past duty stations;

(D) Office or duty telephone number (DOD policy may require withholding of this information in certain circumstances); and

(E) Position descriptions, identification of job elements, and performance standards (but not actual performance appraisals), the release of which would not interfere with law enforcement programs or severely inhibit agency effectiveness. Performance elements and standards (or work expectations) may also be withheld when they are so intertwined with performance appraisals, the disclosure would reveal an individual's performance appraisal.

(d) *Personal information that requires protection.* (1) The following are examples of information that is generally NOT releasable without the written consent of the subject. This list is not all inclusive—

(i) Marital status;

(ii) Dependents' names, sex and SSN numbers;

(iii) Civilian educational degrees and major areas of study (unless the request for the information relates to the professional qualifications for Federal employment);

(iv) School and year of graduation;

(v) Home of record;

(vi) Home address and phone;

(vii) Age and date of birth;

(viii) Overseas assignments (present or future);

(ix) Overseas office or unit mailing address and duty phone of routinely deployable or sensitive units;

(x) Race/ethnic origin;

(xi) Educational level (unless the request for the information relates to professional qualifications for federal employment);

(xii) Social Security Number (SSN); and

(xiii) The information that would otherwise be protected from mandatory disclosure under a FOIA exemption.

(2) The Office of the Secretary of Defense issued a policy memorandum in 2001 that provided greater protection of DOD personnel in the aftermath of 9/11 by requiring information that personally identifies DOD personnel be more carefully scrutinized and limited. In general, the Department of Defense has specifically advised that DOD components are not to release lists of names, duty addresses, present or past position titles, grades, salaries, and performance standards of DOD military members and civilian employees. At the office director level or above, the release of information will be limited to the name, official title, organization, and telephone number, provided a determination is made that disclosure does not raise security or privacy concerns. No other information, including room numbers, will normally be released about these officials. Consistent with current policy, information on officials below the office director level may continue to be released if their positions or duties require frequent interaction with the public.

(3) Disclosure of records pertaining to personnel of overseas, sensitive, or routinely deployed units shall be prohibited to the extent authorized by 10 U.S.C. 130b.

(e) *Release of home addresses and home telephone numbers.* (1) The release of home addresses and home telephone numbers normally is prohibited. This release is normally considered a clearly ''unwarranted invasion'' of personal privacy and is exempt from mandatory release under the FOIA. However, home addresses and home telephone numbers may still be released if—

(i) The individual has indicated previously in writing that he or she has no objection to the release;

(ii) The source of the information to be released is a public document such as commercial telephone directory or other public listing;

(iii) The release is required by Federal statute (for example, pursuant to federally funded state programs to locate parents who have defaulted on child support payments) (See 42 U.S.C. 653); or

(iv) The releasing of information is pursuant to the routine use exception or the ''intra-agency need to know'' exception to the Privacy Act.

(2) A request for a home address or telephone number may be referred to the last known address of the individual for a direct reply by the individual to the requester. In such cases, the requester shall be notified of the referral.

(3) Do not sell or rent lists of individual names and addresses unless such action is specifically authorized by the appropriate authority.

(f) *Emergency Recall Rosters.* (1) The release of emergency recall rosters normally is prohibited. Their release is normally considered a clearly ''unwarranted invasion'' of personal privacy and is exempt from mandatory release under the FOIA. Emergency recall rosters should only be shared with those who have an ''official need to know'' the information, and they should be marked ''For Official Use Only'' (See AR 25–55).

(2) Do not include a person's SSN on an emergency recall roster or their spouse's name.

(3) Commanders and supervisors should give consideration to those individuals with unlisted phone numbers. Commanders and supervisors should consider limiting access to an unlisted number within the unit.

(g) *Social Rosters.* (1) Before including personal information such as a spouse's name, home addresses, home phone numbers, and similar information on social rosters or social directories, which will be shared with individuals, always ask for the individual's written consent. Without their written consent, do not include this information.

(2) Collection of this information will require a Privacy Act Statement which clearly tells the individual what information is being solicited, the purpose, to whom the disclosure of the information is made, and whether collection of the information is voluntary or mandatory.

(h) *Disclosure of personal information on group orders.* (1) Personal information will not be posted on group orders so that everyone on the orders can view it. Such a disclosure of personal information violates the Privacy Act and this part.

(2) The following are some examples of personal information that should not be contained in group orders. The following list is not all-inclusive—

(i) Complete SSN;

(ii) Home addresses and phone numbers; or

(iii) Date of birth.

(i) *Disclosures for established routine uses.* (1) Records may be disclosed outside the DOD without the consent of the individual to whom they pertain for an established routine use.

(2) A routine use shall—

(i) Be compatible with and related to the purpose for which the record was compiled;

(ii) Identify the persons or organizations to which the records may be released; and

(iii) Have been published previously in the **Federal Register**.

(3) Establish a routine use for each user of the information outside the Department of Defense who needs official access to the records.

(4) Routine uses may be established, discontinued, or amended without the consent of the individuals involved. However, new or changed routine uses

must be published in the **Federal Register** at least 30 days before actually disclosing any records.

(5) In addition to the routine uses listed in the applicable systems of records notices, ''Blanket Routine Uses'' for all DOD maintained systems of records have been established. These ''Blanket Routine Uses'' are applicable to every record system maintained within the DOD unless specifically stated otherwise within a particular record system. The ''Blanket Routine Uses'' are listed at appendix C of this part.

(j) *Disclosure accounting.* (1) System managers must keep an accurate record of all disclosures made from DA Privacy Act system of records, including those made with the consent of the individual, except when records are—

(i) Disclosed to DOD officials who have a ''need to know'' the information to perform official government duties; or

(ii) Required to be disclosed under the Freedom of Information Act.

(2) The purpose for the accounting of disclosure is to—

(i) Enable an individual to ascertain those persons or agencies that have received information about them;

(ii) Enable the DA to notify past recipients of subsequent amendments or ''Statements of Dispute'' concerning the record; and

(iii) Provide a record of DA compliance with the Privacy Act of 1974, if necessary.

(3) Since the characteristics of records maintained within DA vary widely, no uniform method for keeping the disclosure accounting is prescribed.

(4) Essential elements to include in each disclosure accounting report are—

(i) The name, position title, and address of the person making the disclosure;

(ii) Description of the record disclosed;

(iii) The date, method, and purpose of the disclosure; and

(iv) The name, position title, and address of the person or agency to which the disclosure was made.

(5) The record subject has the right of access to the disclosure accounting except when—

(i) The disclosure was made for law enforcement purposes under 5 U.S.C. 552a(b)(7); or

(ii) The disclosure was made from a system of records for which an exemption from 5 U.S.C. 552a(c)(3) has been claimed.

(6) There are no approved filing procedures for the disclosure of accounting records; however, system managers must be able to retrieve upon request. With this said, keep disclosure accountings for 5 years after the disclosure, or for the life of the record, whichever is longer.

(7) When an individual requests such an accounting, the system manager or designee will respond within 20 working days.

§ 505.8 Training requirements.

(a) *Training.* (1) The Privacy Act requires all heads of Army Staff agencies, field operating agencies, direct reporting units, Major Commands, 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 non-compliance (See 5 U.S.C. 552a(e)(9)).

(2) To meet the training requirements, three general levels of training must be established. They are—

(i) *Orientation.* Training that provides basic understanding of this part as it applies to the individual's job performance. This training will be provided to personnel, as appropriate, and should be a prerequisite to all other levels of training;

(ii) *Specialized training.* Training that provides information as to the application of specific provisions of this part to specialized areas of job performance. Personnel of particular concern include, but are not limited to, personnel specialists, finance officers, DOD personnel who may be expected to 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 part. Specialized training should be provided on a periodic basis; and

(iii) *Managerial training.* Training designed to identify for responsible managers (such as senior system managers, Denial Authorities, and functional managers described in this section) issues that they should consider when making management decisions affected by the Privacy Act Program.

(b) *Training tools.* Helpful resources include—

(1) Privacy Act training slides for Major Commands and Privacy Act Officers: Contact the DA FOIA/P Office, or slides can be accessed at the Web site *https://www.rmda.belvoir.army.mil/rmdaxml/rmda/FPHomePage.asp.*

(2) The ''DOJ Freedom of Information Act Guide and Privacy Act Overview'': The U.S. Department of Justice, Executive Office for United States Attorneys, Office of Legal Education, 600 E. Street, NW., Room 7600, Washington, DC 20530, or training programs can be accessed at the Web site *www.usdoj.gov/usao/eousa/ole.html.*

§ 505.9 Reporting requirements.

The Department of the Army will submit reports, consistent with the requirements of DOD 5400.11–R, OMB Circular A–130, and as otherwise directed by the Defense Privacy Office. Contact the DA FOIA/P Office for further guidance regarding reporting requirements.

§ 505.10 Use and establishment of exemptions.

(a) *Three types of exemptions.* (1) There are three types of exemptions applicable to an individual's right to access permitted by the Privacy Act. They are the Special, General, and Specific exemptions.

(2) Special exemption (d)(5)—Relieves systems of records from the access provision of the Privacy Act only. This exemption applies to information compiled in reasonable anticipation of a civil action or proceeding.

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

(4) Specific exemptions (k)(1)–(k)(7)–Relieves systems of records from only a few provisions of the Act.

(5) To find out if an exemption is available for a particular record, refer to the applicable system of records notices. System of records notices will state which exemptions apply to a particular type of record. System of records notices that are applicable to the Army are contained in DA Pam 25–51 (available at the Army Publishing Directorate Web site *http://www.usapa.army.mil/*), the Defense Privacy Office's Web site *http://www.defenselink.mil/privacy/*), or in this section). Some of the system of records notices apply only to the Army and the DOD and some notices are applicable government-wide.

(6) Descriptions of current exemptions are listed in detail at appendix C of this part.

(b) *Exemption procedures.* (1) For the General and Specific exemptions to be applicable to the Army, the Secretary of

the Army must promulgate exemption rules to implement them. This requirement is not applicable to the one Special exemption which is self-executing. Once an exemption is made applicable to the Army through the exemption rules, it will be listed in the applicable system of records notices to give notice of which specific types of records the exemption applies to. When a system manager seeks to have an exemption applied to a certain Privacy Act system of records that is not currently provided for by an existing system of records notice, the following information will be furnished to the DA FOIA/P Office—

(i) Applicable system of records notice;

(ii) Exemption sought; and

(iii) Justification.

(2) After appropriate staffing and approval by the Secretary of the Army and the Defense Privacy Office, it will be published in the **Federal Register** as a proposed rule, followed by a final rule 60 days later. No exemption may be invoked until these steps have been completed.

§ 505.11 Federal Register publishing requirements.

(a) *The Federal Register*. There are three types of documents relating to the Privacy Act Program that must be published in the **Federal Register**. They are the DA Privacy Program policy and procedures (AR 340–21), the DA exemption rules, and Privacy Act system of records notices.

(b) *Rulemaking procedures.* (1) DA Privacy Program procedures and exemption rules are subject to the formal rulemaking process.

(2) Privacy Act system of records notices are not subject to formal rulemaking and are published in the **Federal Register** as Notices, not Rules.

(3) The Privacy Program procedures and exemption rules are incorporated into the Code of Federal Regulations (CFR). Privacy Act system of records notices are not published in the CFR.

§ 505.12 Privacy Act enforcement actions.

(a) *Judicial Sanctions.* The Act has both civil remedies and criminal penalties for violations of its provisions.

(1) *Civil remedies.* The DA is subject to civil remedies for violations of the Privacy Act. In addition to specific remedial actions, 5 U.S.C. 552a(g) may provide for the payment of damages, court costs, and attorney's fees.

(2) *Criminal penalties.* A DA official or employee may be found guilty of a misdemeanor and fined not more than $5,000 for willfully—

(i) Disclosing individually identifiable personal information to one not entitled to the information;

(ii) Requesting or obtaining information from another's record under false pretenses; or

(iii) Maintaining a system of records without first meeting the public notice requirements of the Act.

(b) *Litigation Status Sheet.* (1) When a complaint citing the Privacy Act is filed in a U.S. District Court against the Department of the Army, an Army Component, a DA Official, or any Army employee, the responsible system manager will promptly notify the Army Litigation Division, 901 North Stuart Street, Arlington, VA 22203–1837.

(2) The Litigation Status Sheet at appendix E of this part provides a standard format for this notification. At a minimum, the initial notification will have items (a) through (f) provided.

(3) A revised Litigation Status Sheet must be provided at each stage of the litigation.

(4) When a court renders a formal opinion or judgment, copies must be provided to the Defense Privacy Office by the Army Litigation Division.

(c) *Administrative Remedies—Privacy Act complaints.* (1) The installation level Privacy Act Officer 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 Act officer is responsible for—

(i) Reviewing allegations of Privacy Act violations and the evidence provided by the complainants;

(ii) Making an initial assessment as to the validity of the complaint, and taking appropriate corrective action;

(iii) Coordinating with the local Staff Judge Advocate to determine whether a more formal investigation such as a commander's inquiry or an AR 15–6 investigation is appropriate; and

(iv) Ensuring the decision at the local level from either the Privacy Act Officer or other individual who directed a more formal investigation is provided to the complainant in writing.

(2) The decision at the local level may be appealed to the next higher command level Privacy Act Officer.

(3) A legal review from the next higher command level Privacy Act Officer's servicing Staff Judge Advocate is required prior to action on the appeal.

§ 505.13 Computer Matching Agreement Program.

(a) *General provisions.* (1) Pursuant to the Privacy Act and this part, DA records may be subject to computer matching, *i.e.*, the computer comparison of automated systems of records.

(2) There are two specific kinds of Matching Programs covered by the Privacy Act—

(i) Matches using records from Federal personnel or payroll systems of records; and

(ii) Matches involving Federal benefit programs to accomplish one or more of the following purposes—

(A) To determine eligibility for a Federal benefit;

(B) To comply with benefit program requirements; and

(C) To effect recovery of improper payments or delinquent debts from current or former beneficiaries.

(3) The comparison of records must be computerized. Manual comparisons are not covered.

(4) Any activity that expects to participate in a Computer Matching Program must contact the DA FOIA/P Office immediately.

(5) In all cases, Computer Matching Agreements are processed by the Defense Privacy Office and approved by the Defense Data Integrity Board. Agreements will be conducted in accordance with the requirements of 5 U.S.C. 552a, and OMB Circular A–130.

(b) *Other matching.* Several types of computer matching are exempt from the restrictions of the Act such as matches used for statistics, pilot programs, law enforcement, tax administration, routine administration, background checks, and foreign counterintelligence. The DA FOIA/P Office should be consulted if there is a question as to whether the Act governs a specific type of computer matching.

§ 505.14 Recordkeeping requirements under the Privacy Act.

(a) *AR 25–400–2, The Army Records Information Management System (ARIMS).* To maintain privacy records are required by the Army Records Information Management System (ARIMS) to provide adequate and proper documentation of the conduct of Army business so that the rights and interests of individuals and the Federal Government are protected.

(b) A full description of the records prescribed by this part and their disposition/retention requirements are found on the ARIMS Web site at *https://www.arims.army.mil.*

Appendix A to Part 505—References

(a) The Privacy Act of 1974 (5 U.S.C. 552a, as amended).

(b) OMB Circular No. A–130, Management of Federal Information Resources.

(c) AR 25–55, The Department of the Army Freedom of Information Program.

(d) DA PAM 25–51, The Army Privacy Program—System of Records Notices and Exemption Rules.

(e) DOD Directive 5400.11, Department of Defense Privacy Program.

(f) DOD 5400.11–R, Department of Defense Privacy Program.

(g) AR 25–2, Information Assurance

(h) AR 25–400–2, The Army Records Information Management System (ARIMS).

(i) AR 27–10, Military Justice.

(j) AR 40–66, Medical Record Administration and Health Care Documentation.

(k) AR 60–20 and AFR 147–14, Army and Air Force Exchange Service Operating Policies.

(l) AR 190–45, Law Enforcement Reporting.

(m) AR 195–2, Criminal Investigation Activities.

(n) AR 380–5, Department of Army Information Security Program.

(o) DOD Directive 5400–7, DOD Freedom of Information Act (FOIA) Program.

(q) DOD 5400.7–R, DOD Freedom of Information Program.

(r) DOD 6025.18–R, DOD Health Information Privacy Regulation (HIPAA).

(s) U.S. Department of Justice, Freedom of Information Act Guide and Privacy Act Overview.

(t) Office of Secretary of Defense memorandum, dated July 15, 2005, subject: Notifying Individuals when Personal Information is Lost, Stolen, or Compromised located at *http://www.army.mil/ciog6/referencs/policy/dos/OSDprivateinfo.pdf.*

Appendix B to Part 505—Denial Authorities for Records Under Their Authority (Formerly Access and Amendment Refusal Authorities)

(a) The Administrative Assistant to the Secretary of the Army is authorized to act 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 also includes civilian Equal Employment Opportunity (EEO) actions. (*See* DCS, G–1 for Military Equal Opportunity (EO) actions.) The Administrative Assistant to the Secretary of the Army has delegated this authority to the Chief Attorney, OAASA (See DCS, G1 for Military Equal Opportunity (EO) actions).

(b) The Assistant Secretary of the Army (Financial Management and Comptroller) is authorized to act on requests for finance and accounting records. Requests for CONUS finance and accounting records should be referred to the Defense Finance and Accounting Service (DFAS). The Chief Attorney, OAASA, acts on requests for non-finance and accounting records of the Assistant Secretary of the Army (Financial Management and Comptroller).

(c) The Assistant Secretary of the Army (Acquisition, Logistics, & Technology) is authorized to act on requests for procurement records other than those under the purview of the Chief of Engineers and the Commander, U.S. Army Materiel Command. The Chief Attorney, OAASA, acts on requests for non-procurement records of the Assistant Secretary of the Army (Acquisition, Logistics and Technology).

(d) The Deputy Assistant Secretary of the Army (Civilian Personnel Policy)/Director of Civilian Personnel, Office of the Assistant Secretary of the Army (Manpower and Reserve Affairs) is authorized to act 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. The Deputy Assistant Secretary of the Army (Civilian Personnel Policy)/Director of Civilian Personnel has delegated this authority to the Chief, Policy and Program Development Division (**Note:** 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, Assistant Director for Workforce Information, Compliance, and Investigations Group: 1900 E. Street, NW., Washington, DC 20415–0001).

(e) The Chief Information Officer G–6 is authorized to act on requests for records pertaining to Army Information Technology, command, control communications and computer systems and the Information Resources Management Program (automation, telecommunications, visual information, records management, publications and printing).

(f) The Inspector General is authorized to act on requests for all Inspector General Records.

(g) The Auditor General is authorized to act 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.

(h) The Director of the Army Staff is authorized to act 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 Directorate, U.S. Army Resources & Programs Agency (See The Judge Advocate General for the General Officer Management Office actions). The Chief Attorney and Legal Services Director, U.S. Army Resources & Programs Agency acts on requests for records of the Chief of Staff and its Field Operating Agencies (See The Judge Advocate General for the General Officer Management Office actions).

(i) The Deputy Chief of Staff, G–3/5/7 is authorized to act on requests for records relating to International Affairs policy, planning, integration and assessments, strategy formulation, force development, individual and unit training policy, strategic and tactical command and control systems, nuclear and chemical matters, use of DA forces.

(j) The Deputy Chief of Staff, G–8 is authorized to act on requests for records relating to programming, material integration and externally directed reviews.

(k) The Deputy Chief of Staff, G–1 is authorized to act on the following records: Personnel board records, Equal Opportunity (military) and sexual harassment, health promotions, physical fitness and well-being, command and leadership policy records, HIV and suicide policy, substance abuse programs except for individual treatment records which are the responsibility of the Surgeon General, retiree benefits, services, and programs (excluding individual personnel records of retired military personnel, which are the responsibility of the U.S. Army Human Resources Command-St. Louis), DA dealings with Veterans Affairs, U.S. Soldier's and Airmen's Home; all retention, promotion, and separation records; all military education records including records related to the removal or suspension from a military school or class; Junior Reserve Officer Training Corps (JROTC) and Senior Reserve Officer Training Corps (SROTC) records; SROTC instructor records; U.S. Military Academy Cadet Records; recruiting and MOS policy issues, personnel travel and transportation entitlements, military strength and statistics, The Army Librarian, demographics, and Manprint.

(l) The Deputy Chief of Staff, G–4 is authorized to act on requests for records relating to DA logistical requirements and determinations, policy concerning materiel maintenance and use, equipment standards, and logistical readiness.

(m) The Chief of Engineers is authorized to act on requests for records involving civil works, military construction, engineer procurement, and ecology; and the records of the U.S. Army Engineer divisions, districts, laboratories, and field operating agencies.

(n) The Surgeon General/Commander, U.S. Army Medical Command, is authorized to act on requests for medical research and development records, and the 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/test records.

(o) The Chief of Chaplains is authorized to act 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.

(p) The Judge Advocate General is authorized to act on requests for records relating to claims, courts-martial, legal services, administrative

(q) The Chief, National Guard Bureau, is authorized to act 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, operations, and readiness files, policy files, historical files, files relating to National Guard military support, drug interdiction, and civil disturbances; construction, civil works, and ecology records dealing with armories, facilities within the States, ranges, etc.; Equal Opportunity investigative records; aviation program records and financial records dealing with personnel, operation and maintenance, and equipment budgets.

(r) The Chief, Army Reserve and Commander, U.S. Army Reserve Command are authorized to act 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 and the Commander, U.S. Army Reserve Command include records relating to USAR plans, policies, and operations; changes in the organizational status of USAR units; mobilization and demobilization policies, active duty tours, and the Individual Mobilization Augmentation program; and all other Office of the Chief, Army Reserve (OCAR) records and Headquarters, U.S. Army Reserve Command records.

(s) The Commander, United States Army Materiel Command (AMC) is authorized to act on requests for the records of AMC headquarters and to subordinate commands, units, and activities that relate to procurement, logistics, research and development, and supply and maintenance operations.

(t) The Provost Marshal General is authorized to act on all requests for provost marshal activities and law enforcement functions for the Army, all matters relating to police intelligence, physical security, criminal investigations, corrections and internment (to include confinement and correctional programs for U.S. prisoners, criminal investigations, provost marshal activities, and military police support. The Provost Marshal General is responsible for the Office of Security, Force Protection, and Law Enforcement Division and is the functional proponent for AR 190-series (Military Police) and 195-series (Criminal Investigation), AR 630–10 Absent Without Leave, Desertion, and Administration of Personnel Involved in Civilian Court Proceedings, and AR 633–30, Military Sentences to Confinement.

(u) The Commander, U.S. Army Criminal Investigation Command, is authorized to act 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.

(v) The Commander, U.S. Army Human Resources Command, is authorized to act 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 authority.

(w) The Commander, U.S. Army Resources Command-St. Louis has been delegated authority to act on behalf of the U.S. Army Human Resources Commander for 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 authority. The authority does not include records relating to USAR plans, policies, and operations; changes in the organizational status of USAR units, mobilization and demobilization policies; active duty tours, and the individual mobilization augmentation program.

(x) The Assistant Chief of Staff for Installation Management is authorized to act on requests for records relating to planning, programming, execution and operation of Army installations. This includes base realignment and closure activities, environmental activities other than litigation, facilities and housing activities, and installation management support activities.

(y) The Commander, U.S. Army Intelligence and Security Command, is authorized to act on requests for intelligence and security records, foreign scientific and technological records, intelligence training, intelligence threat assessments, and foreign liaison information, mapping and geodesy information, ground surveillance records, intelligence threat assessment, and missile intelligence data relating to tactical land warfare systems.

(z) The Commander, U.S. Army Combat Readiness Center (formerly U.S. Army Safety Center), is authorized to act on requests for Army safety records.

(aa) The Commander, U.S. Army Test and Evaluation Command (ATEC), is authorized to act on requests for the records of ATEC headquarters, its subordinate commands, units, and activities that relate to test and evaluation operations.

(bb) The General Counsel, Army and Air Force Exchange Service, is authorized to act on requests for Army and Air Force Exchange Service records, under AR 60–20/AFR 147–14.

(cc) The Commandant, United States Disciplinary Barracks (USDB) is authorized to act on records pertaining to USDB functional area responsibilities relating to the administration and confinement of individual military prisoners at the USDB. This includes, but is not limited to, all records pertaining to the treatment of military prisoners; investigation of prisoner misconduct; management, operation, and administration of the USDB confinement facility; and related programs which fall directly within the scope of the Commandant's functional area of command and control.

(dd) The Commander, U.S. Army Community and Family Support Center (USACFSC) is authorized to act on requests for records pertaining to morale, welfare, recreation, and entertainment programs; community and family action programs; child development centers; non-appropriated funds issues, and private organizations on Army installations.

(ee) The Commander, Military Surface Deployment and Distribution Command (formerly Military Traffic Management Command) is authorized to act on requests for records pertaining to military and commercial transportation and traffic management records.

(ff) The Director, Installation Management Agency (IMA) is authorized to act on requests for all IMA records.

(gg) Special Denial Authority's authority for time-event related records may be designated on a case-by-case basis. These will be published in the **Federal Register**. You may contact the Department of the Army, Freedom of Information and Privacy Office to obtain current information on special delegations.

Appendix C to Part 505—Privacy Act Statement Format

(a) *Authority:* The specific federal statute or Executive Order that authorizes collection of the requested information.

(b) *Principal Purpose(s):* The principal purpose or purposes for which the information is to be used.

(c) *Routine Uses(s):* Disclosure of the information outside DOD.

(d) *Disclosure:* Whether providing the information is voluntary or mandatory and the effects on the individual if he or she chooses not to provide the requested information.

(1) Example of a Privacy Act Statement

(i) *Authority:* Emergency Supplement Act of 2000; Public Law 106–246; 5 U.S.C. 3013, Secretary of the Army; 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 8013, Secretary of the Air Force; Department of Defense Directive 8500.aa, Information Assurance (IA); and E.O. 9397 (SSN).

(ii) *Principal Purpose(s):* To control access to DOD information, information based systems and facilities by authenticating the identity of a person using a measurable physical characteristic(s). This computer system uses software programs to create biometrics templates and summary statistics, which are used for purposes such as assessing system performance or identifying problem areas.

(iii) *Routine Use(s):* None. The DoD ''Blanket Routine Uses'' set forth at the beginning of the Army's Compilations of System of Records Notices applies to this system.

(iv) *Disclosure:* Voluntary; however, failure to provide the requested information may result in denial of access to DOD information based systems and/or DOD facilities.

(2) [Reserved].

Appendix D to Part 505—Exemptions; Exceptions; and DoD Blanket Routine Uses

(a) *Special Exemption.* 5 U.S.C. 552a(d)(5)—Denies individual access to any information compiled in reasonable anticipation of civil action or proceeding.

(b) *General and Specific Exemptions.* The Secretary of the Army may exempt Army systems of records from certain requirements

of the Privacy Act. The two kinds of exemptions that require Secretary of the Army enactment are General and Specific exemptions. The Army system of records notices for a particular type of record will state whether the Secretary of the Army has authorized a particular General and Specific exemption to a certain type of record. The Army system of records notices are published in DA Pam 25–51 and on the Defense Privacy Office's Web site *http://www.defenselink.mil/privacy/*.

(c) *Twelve Exceptions to the ''No Disclosure without Consent'' rule of the Privacy Act.*

(1) 5 U.S.C. 552a(b)(1)—To DOD officers and employees who have a need for the record in the performance of their official duties. This is the ''official need to know concept.

(2) 5 U.S.C. 552a(b)(2)—FOIA requires release of the information.

(3) 5 U.S.C. 552a(b)(3)—The Routine Use Exception. The Routine Use must be published in the **Federal Register** and the purpose of the disclosure must be compatible with the purpose for the published Routine Use. The applicable Routine Uses for a particular record will be listed in the applicable Army Systems Notice.

(4) 5 U.S.C. 552a(b)(4)—To the Bureau of the Census to plan or carry out a census or survey, or related activity pursuant to Title 13 of the U.S. Code.

(5) 5 U.S.C. 552a(b)(5)—To a recipient who has provided DA or DOD with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable.

(6) 5 U.S.C. 552a(b)(6)—To the National Archives and Records Administration as a record that has sufficient historical or other value to warrant its continued preservation by the U.S. Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value.

Note: Records transferred to the Federal Records Centers for storage remain under the control of the DA and no accounting for disclosure is required under the Privacy Act.

(7) 5 U.S.C. 552a(b)(7)—To another agency or instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity, if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the Army or the DOD specifying the particular portion desired and the law enforcement activity for which the record is sought.

(8) 5 U.S.C. 552a(b)(8)—To a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure, notification is transmitted to the last known address of such individual.

(9) 5 U.S.C. 552a(b)(9)—To either House of Congress, or, to the extent the matter is within its jurisdiction, any committee or subcommittee thereof, or any joint committee of Congress or subcommittee of any such joint committee. Requests from a Congressional member acting on behalf of a constituent are not included in this exception, but may be covered by a routine use exception to the Privacy Act (See applicable Army system of records notice).

(10) 5 U.S.C. 552a(b)(10)—To the Comptroller General or authorized representatives, in the course of the performance of the duties of the Government Accountability Office.

(11) 5 U.S.C. 552a(b)(11)—Pursuant to the order of a court of competent jurisdiction. The order must be signed by a judge.

(12) 5 U.S.C. 552a(b)(12)—To a consumer reporting agency in accordance with section 3711(e) of Title 31 of the U.S. Code. 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. However, before doing so, agencies must complete a series of steps designed to validate the debt and to offer the individual an opportunity to repay it.

(d) *DOD Blanket Routine Uses.* In addition to specific routine uses which are listed in the applicable Army system of record notices, certain ''Blanket Routine Uses'' apply to all DOD maintained systems of records. These are listed on the Defense Privacy Office's Web site *http://www.defenselink.mil/privacy/*. These ''Blanket Routine Uses'' are not specifically listed in each system of records notice as the specific routine uses are. The current DOD ''Blanket Routine Uses'' are as follows—

(1) *Law Enforcement Routine Use.* If a system of records maintained by a DOD component 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 order issued pursuant thereto, 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 statute, rule, regulation or order issued pursuant thereto.

(2) *Disclosure When Requesting Information Routine Use.* A record from a system of records maintained by a DOD component 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 a DOD Component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant or other benefit.

(3) *Disclosure of Requested Information Routine Use.* A record from a system of records maintained by a DOD component 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.

(4) *Congressional Inquiries Disclosure Routine Use.* Disclosure from a system of records maintained by a DOD component 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.

(5) *Private Relief Legislation Routine Use.* Relevant information contained in all systems of records of DOD published on or before August 22, 1975, may be disclosed to Office of Management and Budget 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.

(6) *Disclosures Required by International Agreements Routine Use.* A record from a system of records maintained by a DOD Component may be disclosed to foreign law enforcement, security, investigatory, or administrative authorities in order 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.

(7) *Disclosure to State and Local Taxing Authorities Routine Use.* Any information normally contained in Internal Revenue Service Form W–2, which is maintained in a record from a system of records maintained by a DOD component, may be disclosed to state and local taxing authorities with which the Secretary of the Treasury has entered into agreements pursuant to 5 U.S.C. sections 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 is in accordance with Treasury Fiscal Requirements Manual Bulletin 76–07.

(8) *Disclosure to the Office of Personnel Management Routine Use.* A record from a system of records subject to the Privacy Act and maintained by a DA activity may be disclosed to the Office of Personnel Management concerning information on pay and leave, benefits, retirement deductions, and any other information necessary for Office of Personnel Management to carry out its legally authorized Government-wide personnel management functions and studies.

(9) *Disclosure to the Department of Justice for Litigation Routine Use.* A record from a system of records maintained by a DOD component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee, or member of the Department in pending or potential litigation to which the record is pertinent.

(10) *Disclosure to Military Banking Facilities Overseas Routine Use.* Information as to current military addresses and assignments may be provided to military banking facilities who provide banking services overseas and who are reimbursed by the Government for certain checking and

loan losses. For personnel separated, discharged, or retired from the Armed forces, 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 the individual 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 facility may incur.

(11) *Disclosure of Information to the General Services Administration Routine Use.* A record from a system of records maintained by a DOD component may be disclosed as a routine use to the General Services Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. Sections 2904 and 2906.

(12) *Disclosure of Information to National Archives and Records Administration Routine Use.* A record from a system of records maintained by a DOD component 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 U.S.C. sections 2904 and 2906.

(13) *Disclosure to the Merit Systems Protection Board Routine Use.* A record from a system of records maintained by a DOD component may be disclosed as a routine use to the Merit Systems Protection Board, including 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 U.S.C. sections 1205 and 1206, or as may be authorized by law.

(14) *Counterintelligence Purposes Routine Use.* A record from a system of records maintained by a DOD component 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.

Appendix E to Part 505—Litigation Status Sheet

(a) Case Number: The number used by a DA activity for reference purposes; Requester;

(b) Document Title or Description: Indicates the nature of the case, such as ''Denial of access'', ''Refusal to amend,'' ''Incorrect records'', or other violations of the Act (specify);

(c) Litigation: Date complaint filed, Court, and Case File Number;

(d) Defendants: DOD component and individual;

(e) Remarks: Brief explanation of what the case is about;

(f) Court action: Court's finding and disciplinary action (if applicable); and

(g) Appeal (If applicable): Date complaint filed, court, case File Number, court's finding, disciplinary action (if applicable).

Appendix F to Part 505—Example of a System of Records Notice

(a) Additional information and guidance on Privacy Act system of records notices are found in DA PAM 25–51. The following elements comprise a Privacy Act system of records notice for publication in the **Federal Register:**

(b) *System Identifier:* A0025–55 AHRC—DA FOIA/P Office assigns the notice number, for example, A0025–55, where ''A'' indicates ''Army,'' the next number represents the publication series number related to the subject matter, and the final letter group shows the system manager's command. In this case, it would be U.S. Army Human Resources Command.

(c) *System Name:* Use a short, specific, plain language title that identifies the system's general purpose (limited to 55 characters).

(d) *System Location:* Specify the address of the primary system and any decentralized elements, including automated data systems with a central computer facility and input or output terminals at separate locations. Use street address, 2-letter state abbreviations and 9-digit ZIP Codes. Spell out office names. Do not use office symbols.

(e) *Categories of Individuals:* Describe the individuals covered by the system. Use non-technical, specific categories of individuals about whom the Department of Army keeps records. Do not use categories like ''all Army personnel'' unless that is truly accurate.

(f) *Categories of Records in the System:* Describe in clear, plain language, all categories of records in the system. List only documents actually kept in the system. Do not identify source documents that are used to collect data and then destroyed. Do not list form numbers.

(g) *Authority for Maintenance of the System:* Cite the specific law or Executive Order that authorizes the maintenance of the system. Cite the DOD directive/instruction or Department of the Army Regulation(s) that authorizes the Privacy Act system of records. Always include titles with the citations. Note: Executive Order 9397 authorizes using the SSN as a personal identifier. Include this authority whenever the SSN is used to retrieve records.

(h) *Purpose(s):* List the specific purposes for maintaining the system of records by the activity.

(i) *Routine Use(s):* The blanket routine uses that appear at the beginning of each Component compilation apply to all systems notice unless the individual system notice specifically states that one or more of them do not apply to the system. Blanket Routine Uses are located at the beginning of the Component listing of systems notices and are not contained in individual system of records notices. However, specific routine uses are listed in each applicable system of records notice. List the specific activity to which the record may be released, for example ''To the Veterans Administration'' or ''To state and local health agencies''. For each routine user identified, include a statement as to the purpose or purposes for which the record is to release to that activity. Do not use general statements, such as ''To other federal agencies as required'' or ''To any other appropriate federal agency''.

(j) *Polices and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:*

(k) *Storage:* State the medium in which DA maintains the records; for example, in file folders, card files, microfiche, computer, or a combination of those methods. Storage does not refer to the storage container.

(l) *Retrievability:* State how the Army retrieves the records; for example, by name, fingerprints or voiceprints.

(m) *Safeguards:* Identify the system safeguards; for example, storage in safes, vaults, locked cabinets or rooms, use of guards, visitor controls, personnel screening, computer systems software, and so on. Describe safeguards fully without compromising system security.

(n) *Retention and Disposal.* State how long AR 25–400–2 requires the activity to maintain the records. Indicate when or if the records may be transferred to a Federal Records Center and how long the record stays there. Specify when the Records Center sends the record to the National Archives or destroys it. Indicate how the records may be destroyed.

(o) *System Manager(s) and Address:* List the position title and duty address of the system manager. For decentralized systems, show the locations, the position, or duty title of each category of officials responsible for any segment of the system.

(p) *Notification Procedures:* List the title and duty address of the official authorized to tell requesters if their records are in the system. Specify the information a requester must submit; for example, full name, military status, SSN, date of birth, or proof of identity, and so on.

(q) *Record Access Procedures:* Explain how individuals may arrange to access their records. Include the titles or categories of officials who may assist; for example, the system manager.

(r) *Contesting Records Procedures:* The standard language to use is ''The Army's rules for accessing records, and for contesting contents and appealing initial agency determinations are contained in Army Regulation 25–71; 32 CFR part 505; or may be obtained from the system manager.''

(s) *Record Source Categories:* Show categories of individuals or other information sources for the system. Do not list confidential sources protected by 5 U.S.C. 552a(k)(2), (k)(5), or (k)(7).

(t) *Exemptions Claimed for the System:* Specifically list any approved exemption including the subsection in the Act. When a system has no approved exemption, write ''none'' under this heading.

Appendix G to Part 505—Management Control Evaluation Checklist

(a) *Function.* The function covered by this checklist is DA Privacy Act Program.

(b) *Purpose.* The purpose of this checklist is to assist Denial Authorities and Activity Program Coordinators in evaluating the key management controls listed below. This checklist is not intended to cover all controls.

(c) *Instructions.* Answer should be based on the actual testing of key management controls (e.g., document analysis, direct observation, sampling, simulation, other). Answers that indicate deficiencies should be explained and corrective action indicated in supporting documentation. These management controls must be evaluated at least once every five years. Certificate of this evaluation has been conducted and should be accomplished on DA Form 11–2–R (Management Control Evaluation Certification Statement).

Test Questions

a. Is a Privacy Act Program established and implemented in your organization?

b. Is an individual appointed to implement the Privacy Act requirements?

c. Are provisions of AR 25–71 concerning protection of OPSEC sensitive information regularly brought to the attention of managers responsible for responding to Privacy Act requests and those responsible for control of the Army's records?

d. When more than twenty working days are required to respond, is the Privacy Act requester informed, explaining the circumstance requiring the delay and provided an appropriate date for completion.

e. Are Accounting Disclosures Logs being maintained?

Comments: Assist in making this a better tool for evaluating management controls. Submit comments to the Department of Army, Freedom of Information and Privacy Division.

Appendix H to Part 505—Definitions

Function

(a) *Access.* Review or copying a record or parts thereof contained in a Privacy Act system of records by an individual.

(b) *Agency.* For the purposes of disclosing records subject to the Privacy Act, Components of the Department of Defense are considered a single agency. For other purposes including access, amendment, appeals from denials of access or amendment, exempting systems of records, and recordkeeping for release to non-DOD agencies, the Department of the Army is considered its own agency.

(c) *Amendment.* The process of adding, deleting, or changing information in a system of records to make the data accurate, relevant, timely, or complete.

(d) *Computer Matching Agreement.* An agreement to conduct a computerized comparison of two or more automated systems of records to verify eligibility for payments under Federal benefit programs or to recover delinquent debts for these programs.

(e) *Confidential Source.* A person or organization who has furnished information to the Federal Government under an express promise that the person's or the organization's identity would be held in confidence or under an implied promise of such confidentiality if this implied promise was made before September 27, 1975.

(f) *Cookie.* A mechanism that allows the server to store its own information about a user on the user's own computer. Cookies are embedded in the HTML information flowing back and forth between the user's computer and the servers. They allow user-side customization of Web information. Normally, cookies will expire after a single session.

(g) *Defense Data Integrity Board.* The Board oversees and coordinates all computer matching programs involving personal records contained in systems of records maintained by the DOD Component; reviews and approves all computer matching agreements between the Department of Defense (DOD) and other Federal, State, and local governmental agencies, as well as memoranda of understanding when the match is internal to the DOD.

(h) *Disclosure.* The transfer of any personal information from a Privacy Act system of records by any means of communication (such as oral, written, electronic mechanical, or actual review) to any persons, private entity, or government agency, other than the subject of the record, the subject's designated agent or the subject's legal guardian. Within the context of the Privacy Act and this part, this term applies only to personal information that is a part of a Privacy Act system of records.

(i) *Deceased Individuals.* The Privacy Act confers no rights on deceased persons, nor may their next-of-kin exercise any rights for them. However, family members of deceased individuals have their own privacy right in particularly sensitive, graphic, personal details about the circumstances surrounding an individual's death. This information may be withheld when necessary to protect the privacy interests of surviving family members. Even information that is not particularly sensitive in and of itself may be withheld to protect the privacy interests of surviving family members if disclosure would rekindle grief, anguish, pain, embarrassment, or cause a disruption of their peace minds. Because surviving family members use the deceased's Social Security Number to obtain benefits, DA personnel should continue to protect the SSN of deceased individuals.

(j) *Individual.* A living person who is a citizen of the United States or an alien lawfully admitted for permanent residence. The parent or legal guardian of a minor also may act on behalf of an individual. Members of the United States Armed Forces are individuals. Corporations, partnerships, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities are not individuals.

(k) *Individual Access.* The subject of a Privacy Act file or his or her designated agent or legal guardian has access to information about them contained in the Privacy Act file. The term individual generally does not embrace a person acting on behalf of a commercial entity (for example, sole proprietorship or partnership).

(l) *Denial Authority (formerly Access and Amendment Refusal Authority).* The Army Staff agency head or major Army commander designated authority by this part to deny access to, or refuse amendment of, records in his or her assigned area or functional specialization.

(m) *Maintain.* Includes keep, collect, use or disseminate.

(n) *Members of the Public.* Individuals or parties acting in a private capacity.

(o) *Minor.* An individual under 18 years of age, who is not married and who is not a member of the Department of the Army.

(p) *Official Use.* Within the context of this part, this term is used when Department of the Army officials and employees have demonstrated a need for the use of any record or the information contained therein in the performance of their official duties.

(q) *Personal Information.* Information about an individual that identifies, relates, or is unique to, or describes him or her, e.g., a social security number, age, military rank, civilian grade, marital status, race, salary, home/office phone numbers, etc.

(r) *Persistent cookies.* Cookies that can be used to track users over time and across different Web sites to collect personal information.

(s) *Personal Identifier.* A name, number, or symbol that is unique to an individual, usually the person's name or SSN.

(t) *System of Records.* A group of records under the control of the DA from which information is filed and retrieved by individuals' names or other personal identifiers assigned to the individuals. System notices for all systems of records must be published in the **Federal Register**. A grouping of records arranged chronologically or subjectively that are not retrieved by individuals' names or identifiers is not a Privacy Act system of records, even though individual information could be retrieved by individuals' names or personal identifiers, such as through a paper-by-paper search.

(u) *Privacy Advisory.* A statement required when soliciting personally identifying information by a Department of the Army Web site and the information is not maintained in a system of records. The Privacy Advisory informs the individual why the information is being solicited and how it will be used.

(v) *Privacy Impact Assessment (PIA).* An analysis, which considers information sensitivity, vulnerability, and cost to a computer facility or word processing center in safeguarding personal information processed or stored in the facility.

(w) *Privacy Act (PA) Request.* A request from an individual for information about the existence of, access to, or amendment of records pertaining to that individual located in a Privacy Act system of records. The request must cite or implicitly refer to the Privacy Act of 1974.

(x) *Protected Personal Information.* Information about an individual that identifies, relates to, is unique to, or describes him or her (e.g., home address, date of birth, social security number, credit card, or charge card account, etc.).

(y) *Records.* Any item, collection, or grouping of information, whatever the storage media (e.g., paper, electronic, etc), about an individual that is maintained by a DOD Component, including but not limited to, his or her education, financial transactions, medical history, criminal or employment history and that contains his or her name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

(z) *Records Maintenance and Use.* Any action involving the storage, retrieval, and handling of records kept in offices by or for the agency.

(aa) *Review Authority.* An official charged with the responsibility to rule on administrative appeals of initial denials of requests for notification, access, or amendment of records. Additionally, the Office of Personnel Management is the review authority for civilian official personnel folders or records contained in any other OMP record.

(bb) *Routine Use.* Disclosure of a record outside DOD 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. A routine use must be included in the notice for the Privacy Act system of records published in the **Federal Register**.

(cc) *Statistical record.* A record in a system of records maintained for statistical research or reporting purposes and not used in whole or in part in making determinations about specific individuals.

(dd) *System Manager.* An official who has overall responsibility for policies and procedures for operating and safeguarding a Privacy Act system of records.

(ee) *Third-party cookies.* Cookies placed on a user's hard drive by Internet advertising networks. The most common third-party cookies are placed by the various companies that serve the banner ads that appear across many Web sites.

(ff) *Working Days.* Days excluding Saturday, Sunday, and legal holidays.

[FR Doc. 06–6799 Filed 8–9–06; 8:45 am]

BILLING CODE 3710–08–P