

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 al-

tered 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.defenseink.mil/privacy>.

#### § 505.4

#### 32 CFR Ch. V (7-1-09 Edition)

(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.