

(2) Since the characteristics of records maintained within the Army vary widely, no uniform method for keeping the disclosure of accounting is prescribed. For most paper records, the accounting may be affixed to the record being disclosed. It must be a written record and consist of:

- (i) Description of the record disclosed;
- (ii) Name, position title, and address of the person to whom disclosure was made;
- (iii) Date, method, and purpose of the disclosure; and
- (iv) Name and position title of the person making the disclosure.

(3) Purpose of the accounting of disclosure is to enable an individual:

- (i) To ascertain those persons/agencies that have received information about the individual, and
- (ii) To provide a basis for informing recipients of subsequent amendments or statements of dispute concerning the record.

(4) When an individual requests such an accounting, the system manager or designee shall respond within 10 work days and inform the individual of the items in § 505.3(d)(2) above.

(5) The only basis for not furnishing the data subject an accounting of disclosures are if disclosure was made for law enforcement purposes under 5 U.S.C. 552a(b)(7), or the disclosure was from a system of records for which an exemption from 5 U.S.C. 552a(c)(3) has been claimed (see appendix C to this part).

[50 FR 42164, Oct. 18, 1985, as amended at 58 FR 51013, Sept. 30, 1993]

**§ 505.4 Record-keeping requirements under the Privacy Act.**

(a) *Systems of records.* (1) Notices of all Army systems of records are required by the Act to be published in the FEDERAL REGISTER. An example is at appendix A to this part. When new systems are established, or major changes occur in existing systems, which meet the criteria of OMB Guidelines summarized at § 505.4(f)(2), advance notice is required to be furnished OMB and the Congress before the system or proposed changes become operational.

(2) Uncirculated personal notes, papers and records which are retained at the author's discretion and over which the Army exercises no control or dominion are not considered Army records within the meaning of the Privacy Act. Individuals who maintain such notes must restrict their use of memory aids. Disclosure from personal notes, either intentional or through carelessness, remove the information from the category of memory aids and the notes then become subject to the provisions of the Act.

(3) Only personal information as is relevant and necessary to accomplish a purpose or mission of the Army, required by Federal statute or Executive Order of the President, will be maintained in Army systems of records. Statutory authority, or regulatory authority to establish and maintain a system of records does not convey unlimited authority to collect and maintain all information which may be useful or convenient. The authority is limited to relevant and necessary information.

(4) Except for statistical records, most records could be used to determine an individual's rights, benefits, or privileges. To ensure accuracy, personal information to be included in a system of records will be collected directly from the individual if possible. Collection of information from third parties should be limited to verifying information for security or employment suitability or obtaining performance data or opinion-type evaluations.

(b) *Privacy Act Statement.* Whenever personal information is requested from an individual that will become part of system of records retrieved by reference to the individual's names or other personal identifier, the individual will be furnished a Privacy Act Statement. This is to ensure that individuals know why the information is collected so they can make an informed decision on whether or not to furnish it. As a minimum, the Privacy Act Statement will include the following information in language that is explicit and easily understood and not so lengthy as to deter an individual from reading it:

(1) Cite the specific statute or Executive Order, including a brief title or

subject, that authorizes the Army to collect the personal information requested. Inform the individual whether or not a response is mandatory or voluntary, and any possible consequences of failing to respond.

(2) Cite the principal purpose(s) for which the information will be used; and

(3) Cite the probable routine uses for which the information may be used.

This may be a summary of information published in the applicable system notice. The above information normally should be printed on the form used to record the information. In certain instances, it may be printed in a public notice in a conspicuous location such as check-cashing facilities; however, if the individual requests a copy of its contents, it must be provided.

(c) *Social Security Number (SSN)*. Executive Order 9397 authorizes the Department of the Army to use the SSN as a system of identifying Army members and employees. Once a military member or civilian employee of the Department of the Army has disclosed his/her SSN for purposes of establishing personnel, financial, or medical records upon entry into Army service or employment, the SSN becomes his/her identification number. No other use of this number is authorized. Therefore, whether the SSN alone is requested from the individual, or the SSN together with other personal information, the Privacy Act Statement must make clear that disclosure of the number is voluntary. If the individual refuses to disclose his/her SSN, the Army activity must be prepared to identify the individual by alternate means.

(d) *Safeguarding personal information*. (1) The Privacy Act requires establishment of appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any threats or hazards to the subjects security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness.

(2) At each location, and for each system of records, an official will be designated to safeguard the information in that system. Consideration must be given to sensitivity of the data, need for accuracy and reliability in oper-

ations, general security of the area, cost of safeguards, etc. See AR 380-380.

(3) Ordinarily, personal information must be afforded at least the protection required for information designated "For Official Use Only" (see Chapter IV, AR 340-17). Privacy Act data will be afforded reasonable safeguards to prevent inadvertent or unauthorized disclosure of record content during processing, storage, transmission, and disposal.

(4) No comparisons of Army records systems with systems of other Federal or commercial agencies (known as "matching" or "computer matching" programs) will be accomplished without prior approval of the Assistant Chief of Staff for Information Management (DAIM-RMS-S), Alex, VA 22331-0301.

(e) First Amendment rights. No record describing how an individual exercises rights guaranteed by the First Amendment will be kept unless expressly authorized by Federal statute, by the individual about whom the record pertains, or unless pertinent to and within the scope of an authorized law enforcement activity. Exercise of these rights includes, but is not limited to, religious and political beliefs, freedom of speech and the press, and the right of assembly and to petition.

(f) *System notice*. (1) The Army publishes in the FEDERAL REGISTER a notice describing each system of records for which it is responsible. A notice contains:

(i) Name and location(s) of the records;

(ii) Categories of individuals on whom records are maintained;

(iii) Categories of records in the system;

(iv) Authority (statutory or Executive Order) authorizing the system;

(v) Purpose(s) of the system;

(vi) Routine uses of the records, including the categories of users and the purposes of such uses;

(vii) Policies and practices for storing, retrieving, accessing, retaining, and disposing of the records;

(viii) Position title and business address of the responsible official;

(ix) Procedures an individual must follow to learn if a system of records contains a record about the individual;

(x) Procedures an individual must follow to gain access to a record about that individual in a system of records, to contest contents, and to appeal initial determinations;

(xi) Categories of sources of records in the system;

(xii) Exemptions from the Privacy Act claimed for the system. (See example notice at appendix A to this part.)

(2) New, or altered, systems which meet the requirements below, require a report to the Congress and the Office of Management and Budget. A new system is one for which no system notice is published in the FEDERAL REGISTER. An altered system is one that:

(i) Increases or changes the number or types of individuals on whom records are kept so that it significantly alters the character and purpose of the system of records.

(ii) Expands the types of categories of information maintained.

(iii) Alters the manner in which records are organized, indexed, or retrieved so as to change the nature or scope of those records.

(iv) Alters the purposes for which the information is used, or adds a routine use that is not compatible with the purpose for which the system is maintained.

(v) Changes the equipment configuration on which the system is operated so as to create potential for either greater or easier access.

(3) Report of a new or altered system must be sent to HQDA (DAIM-RMS-S) at least 120 days before the system or changes become operational, and include a narrative statement and supporting documentation.

(i) The narrative statement must contain the following items:

(A) System identification and name;

(B) Responsible official;

(C) Purpose(s) of the system, or nature of changes proposed (if an altered system);

(D) Authority for the system;

(E) Number (or estimate) of individuals on whom records will be kept;

(F) Information of First Amendment activities;

(G) Measure to assure information accuracy;

(H) Other measures to assure system security; (Automated systems require risk assessment under AR 380-380.)

(I) Relations to State/local government activities. (See example at appendix B to this part.)

(4) Supporting documentation consists of system notice for the proposed new or altered system, and proposed exemption rule, if applicable.

(g) *Reporting requirements.* (1) The annual report required by the Act, as amended by Pub. L. 97-375, 96 Stat. 1821, focuses on two primary areas:

(i) Information describing the exercise of individuals' rights of access to and amendment of records.

(ii) Changes in, or additions to, systems of records.

(2) Specific reporting requirements will be disseminated each year by The Assistant Chief of Staff for Information Management (DAIM-RMS-S) in a letter to reporting elements.

(h) *Rules of conduct.* System managers will ensure that all personnel, including government contractors or their employees, who are involved in the design, development, operation, maintenance, or control of any system of records, are informed of all requirements to protect the privacy of individuals who are subjects of the records.

(i) *Judicial sanctions.* The Privacy Act has both civil remedies and criminal penalties for violations of its provisions:

(1) Civil remedies: An individual may file a civil suit against the Army if Army personnel fail to comply with the Privacy Act.

(2) Criminal penalties: A member or employee of the Army may be guilty of a misdemeanor and fined not more than \$5,000 for willfully:

(i) Maintaining a system of records without first meeting the public notice requirements of publishing in the FEDERAL REGISTER;

(ii) Disclosing individually identifiable personal information to one not entitled to have it;

(iii) Asking for or getting another's record under false pretense.

#### § 505.5 Exemptions.

(a) *Exempting systems of records.* The Secretary of the Army may exempt Army systems of records from certain