

(ii) Retrieving by SSNs records that previously were retrieved only by names would be an alteration if the present notice failed to indicate retrieval by SSNs.

(c) *Reports of new and altered systems of records.* (1) Under subsection (o) of the Privacy Act, reports of new and altered systems of records must be submitted to Congress and the Office of Management and Budget.

(2) The agency shall submit reports of new or altered systems to the Defense Privacy Office, DA&M, before collecting information for new systems or altering an existing system.

(3) The Defense Privacy Office, DA&M, shall coordinate all reports of new or altered systems with the Office of the Assistant Secretary of Defense (Legislative Affairs) and the Office of the General Counsel, Department of Defense.

(4) The Defense Privacy Office, DA&M, shall prepare, for the approval and signature of the Director, Administration and Management, Office of the Secretary of Defense, transmittal letters to Congress and the Office of Management and Budget.

(d) *Time limits before implementing routine uses.* After publishing a system notice in the FEDERAL REGISTER, 30 days must elapse before routine uses may be employed.

**§ 317.74 Amendment and deletion of system notices.**

(a) *Criteria for an amended record system.* Minor changes to published system notices are considered amendments rather than alterations. Amendments must also be published in the FEDERAL REGISTER, but a new or altered system report does not have to be accomplished.

(b) *Amending a system notice.* In submitting an amendment to a system notice for publication in the FEDERAL REGISTER, the agency must include:

(1) The system identification and name.

(2) A description of the specific changes proposed; and

(3) The full text of the system notice as amended.

(c) *Deleting a system notice.* (1) When a system of records is discontinued, in-

corporated into another system, or determined to be no longer subject to this rule, a deletion notice must be published in the FEDERAL REGISTER.

(2) The deletion notice shall include:

(i) The system identification number and name.

(ii) The FEDERAL REGISTER citation of the latest publication of the system.

(iii) The reason for the deletion.

(3) If a system is deleted through combination or merger with another system, identify the successor system in the deletion notice.

(d) *Submitting amendments and deletions for publication.* (1) Amendments and deletions should be submitted through the agency Privacy Advisor to the Defense Privacy Office, DA&M, which will transmit them to the FEDERAL REGISTER for publication.

(2) At least one original in proper format should be included in the submission.

(3) Multiple amendments and deletions, and combinations of amendments and deletions, may be submitted together.

**Subpart H—Training Requirements**

**§ 317.80 Statutory training requirements.**

(a) *Establishing rules of conduct.* Under subsection (e)(9) of the Privacy Act, the agency is required to establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record.

(b) *Training.* The agency shall train all personnel involved in the functions described in the preceding paragraph. The training shall include instruction in the rules of conduct and all requirements prescribed by the Privacy Act, including the penalties for noncompliance.

**§ 317.81 DCAA training programs.**

(a) *Personnel to be trained.* (1) To conform with Office of Management and Budget guidance, compliance with the statutory training requirements requires informed and active support of all agency personnel. All personnel who in any way use or operate systems of

records, or who are engaged in the development of procedures for handling records, must be taught the requirements of the Privacy Act and must be trained in the agency's procedures for the implementation of the Privacy Act.

(2) Personnel to be trained include, but are not limited to, those engaged in the following:

- (i) Personnel management.
- (ii) Personnel finance.
- (iii) Medical care.
- (iv) Investigations of personnel.
- (v) Records management (reports, forms, records, and related functions).
- (vi) Computer systems development and operation.
- (vii) Communications.
- (viii) Statistical data collection and analysis, and
- (ix) Performing other functions subject to this rule.

(b) *Types of training.* The agency shall establish the following three levels of training for those persons who are involved with the design, development, operation, or maintenance of any system of records. The training shall be provided to persons before or shortly after assuming the duties associated with the level of involvement.

(1) *Orientation training.* Orientation training that provides a general understanding of the individual's rights under the Privacy Act.

(2) *Specialized training.* Training concerning the application of this part to specialized areas of job performance.

(3) *Management training.* Training concentrated on factors affecting decisions made by managers under the Privacy Program, such as system managers, denial authorities, and managers of the specific functions listed.

(c) *Methods of training.* The agency is responsible for developing training methods that will meet this criteria. Such methods may include formal and informal (on-the-job) programs, if those personnel giving the training have, themselves, been trained.

### Subpart I—Computer Matching Program Procedures

#### §317.90 General.

(a) *Scope.* The Privacy Act and this rule are applicable to certain types of

computer matching--the computer comparison of automated systems of records.

(b) *Compliance.* Although the Privacy Act provides for specific procedures, the Act is not in itself authority for carrying out any matching activity. Compliance with this chapter does not relieve the agency of the obligation to comply with any other requirements of the Privacy Act and this part.

(c) *Matching programs covered by the Privacy Act.* There are two specific kinds of matching programs that are fully governed by the Privacy Act and this part. These are:

(1) Matches using records from Federal personnel or payroll systems of records. See also definitions of this part.

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

(i) To determine eligibility for a Federal benefit.

(ii) To comply with benefit program requirements.

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

(d) *Automated comparisons.* The record comparison must be a computerized comparison, manual comparisons are not covered, involving records from:

(1) Two or more automated systems of records (i.e., systems of records maintained by Federal agencies that are subject to the Privacy Act); or,

(2) An agency's automated system of records and automated records maintained by a non-Federal agency (i.e., state or local government or agent thereof).

(e) *Features of a matching program.* A covered computer matching program entails not only the actual computerized comparison, but also preparing and executing a written agreement between the participants, securing approval of the Defense Data Integrity Board, publishing a matching notice in the FEDERAL REGISTER before the match begins, ensuring that investigation and due process are completed, and taking ultimate action, if any.