

§317.6

(D) Conduct training on the Privacy Act program for regional and FAO personnel.

(E) Provide recommendations to the Regional Director through the Regional Resources Manager regarding the releasability of DCAA records to members of the public.

(6) *Managers, Field Audit Offices (FAOs)* will:

(i) Ensure that the provisions of this part are followed in processing requests for records.

(ii) Forward to the Regional Privacy Act Officer, any Privacy Act requests received directly from a member of the public, so that the request may be administratively controlled and processed.

(iii) Ensure the prompt review of all Privacy Act requests, and when required, coordinating those requests with other organizational elements.

(iv) Provide recommendations to the Regional Privacy Act Officer regarding the releasability of DCAA records to members of the public, along with the responsive documents.

(v) Provide the appropriate documents, along with a written justification for any denial, in whole or in part, of a request for records to the Regional Privacy Act Officer. Those portions to be excised should be bracketed in red pencil, and the specific exemption or exemptions cited which provide the basis for denying the requested records.

(7) *DCAA Employees* will:

(i) Not disclose any personal information contained in any system of records, except as authorized by this part.

(ii) Not maintain any official files which are retrieved by name or other personal identifier without first ensuring that a notice for the system has been published in the FEDERAL REGISTER.

(iii) Report any disclosures of personal information from a system of records or the maintenance of any system of records that are not authorized by this part to the appropriate Privacy Act officials for their action.

§317.6 Procedures.

Procedures for processing material in accordance with the Privacy Act of

32 CFR Ch. I (7-1-99 Edition)

1974 are outlined in subparts B through L of this part.

Subpart B—Systems of Records

§317.10 General.

(a) *System of records.* To be subject to this part, a "system of records" must:

(1) Consist of "records" that are retrieved by the name or some other personal identifier of an individual, and

(2) Be under the control of the Agency.

(b) *Retrieval practices.* (1) Records in a group of records that could be retrieved by personal identifiers, but are not covered by this part, even if the records contain information about individuals and are under the control of the agency. The records must, in fact, be retrieved by personal identifiers in order to become a system of records.

(2) If records previously not retrieved by personal identifiers are rearranged so they are retrieved by personal identifiers, a new system of records is created and a notice of the system must be published in the FEDERAL REGISTER of its existence.

(3) If records in a system of records are rearranged so retrieval no longer is by personal identifiers, the records are no longer subject to this part and the records system notice shall be deleted.

(c) *Recordkeeping standards.* A record maintained in a system of records must meet the following criteria:

(1) The record must be accurate--all information in the record must be factually correct.

(2) The record must be relevant--all information contained in the record must be related to the individual who is the subject of record and also must be related to a lawful purpose or mission of the agency.

(3) The record must be timely--all information in the record must be reviewed periodically to ensure that it has not changed due to time or later events.

(4) The record must be complete--it must be able to stand alone in accomplishing the purpose for which it is maintained.

(5) The record must be necessary--all information in the record must be

needed to accomplish the agency mission or purpose established by Federal law or Executive Order of the President.

(d) *Authority to establish systems of records.* The specific Federal statute or Executive Order of the President should be identified that authorizes maintaining each system of records. A statute or Executive Order authorizing a system of records does not negate the responsibility to ensure the information in the system of records is relevant and necessary.

(e) *Exercise of first amendment rights.*

(1) Records should not be maintained describing how an individual exercises rights guaranteed by the first amendment of the U.S. Constitution unless:

(i) Expressly authorized by Federal law;

(ii) Expressly authorized by the individual; or

(iii) Pertinent to and within the scope of an authorized law enforcement activity.

(2) First amendment rights include, but are not limited to, freedom of religion, freedom of political beliefs, freedom of speech, freedom of the press, the right to assemble, and the right to petition.

(f) *System manager's evaluations and reviews.* (1) Each new proposed system of records shall be evaluated.

(i) The information to be included in the system should be evaluated before establishing it.

(ii) The following factors should be considered:

(A) The relationship of each item of information to be collected and retained to the purpose for which the system is maintained. All information must be relevant to the purpose.

(B) The specific impact on the purpose or mission if each category of information is not collected. All information must be necessary to accomplish a lawful purpose or mission.

(C) The ability to meet the informational needs without using personal identifiers (will anonymous statistical records meet the needs?).

(D) The length of time each item of information must be kept.

(E) The methods of disposal; and

(F) The cost of maintaining the information.

(2) All existing systems of records shall be evaluated and reviewed.

(i) When an alteration or amendment of an existing system is prepared, an evaluation must be performed.

(ii) Reviews should be conducted often and reports prepared which outline the results and corrective actions taken to resolve problems uncovered.

(A) Training practices should be reviewed annually to ensure all personnel are familiar with the requirements of the Privacy Act and any special needs their specific jobs entail.

(B) Recordkeeping and disposal practices should be reviewed annually to ensure compliance with this part.

(C) Each ongoing computer matching program in which records from the system have been matched with non-DoD records should be reviewed annually to ensure that the applicable requirements have been met.

(D) Actions of agency personnel that resulted in either the agency being found civilly liable or an employee being found criminally liable should be reviewed annually to determine the extent of the problem and find the most effective way of preventing the problem in the future.

(E) Each system of records notice should be reviewed annually to ensure it accurately describes the system. Where minor changes are needed, amend the system notice. If major changes are needed, alter the system notice.

(F) A random sample of agency contracts that provide for the operation of a system of records on behalf of the agency to accomplish an agency function should be reviewed every even-numbered year to ensure the wording of each contract complies with the provisions of the Privacy Act of 1974 (5 U.S.C. 552a).

(G) The routine use disclosures associated with each system of records should be reviewed every three years to ensure the recipient's use of the records continues to be compatible with the purpose for which the agency originally collected the information.

(H) Each system of records for which exemption rules have been established should be reviewed every three years to determine whether each exemption is still needed.

§317.11

(iii) When directed, the reports should be sent through proper channels to the agency Privacy Act Advisor who will forward them to the Defense Privacy Office.

(g) *Discontinued information requirements.* (1) Any category or item of information about individuals that is no longer justified should not be collected, and when feasible, the information should be removed from existing records.

(2) Records that must be kept in accordance with retention and disposal needs established under DCAA Manual 5015.1⁶, "Files and Disposition Manual," shall not be destroyed.

(h) *Review records before disclosing them outside the Federal government.* Before disclosing a record from a system of records to anyone outside the Federal government, reasonable steps should be taken to ensure the record to be disclosed is accurate, relevant, timely, and complete for the purposes it is being maintained.

§317.11 Federal Government contractors.

(a) *Applicability to Federal government contractors.* (1) When the agency contracts for the operation of a system of records or portion thereof to accomplish an agency function, this part and 5 U.S.C. 552a are applicable. For purposes of the criminal penalties, the contractor and its employees shall be considered employees of the agency during the performance of the contract.

(2) Consistent with Parts 24 and 52 of the Federal Acquisition Regulation⁷, contracts for the operation of a system of records or portion thereof shall identify specifically the record system and the work to be performed, and shall include in the solicitations and resulting contract such terms specifically prescribed by the FAR.

(3) If the contractor must use records that are subject to this part to perform any part of a contract, and the information would have been collected and maintained by the agency but for the

⁶See footnote 1 to §317.1(a).

⁷For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402.

32 CFR Ch. I (7-1-99 Edition)

contract, the contractor activities are subject to this rule.

(4) This rule does not apply to records of a contractor that are:

(i) Established and maintained solely to assist the contractor in making internal contractor management decisions, such as records maintained by the contractor for use in managing the contract; or

(ii) Maintained as internal contractor employee records, even when used in conjunction with providing goods or services to the agency.

(iii) For contracting that is subject to this part, the agency shall:

(A) Inform prospective contractors of their responsibilities under the DCAA Privacy Program.

(B) Establish an internal system for reviewing contractor performance to ensure compliance with the DCAA Privacy Program; and

(C) Provide for the biennial review of a random sampling of agency contracts that are subject to this rule.

(b) *Contracting procedures.* The Defense Acquisition Regulatory Council is responsible for developing the specific policies and procedures for soliciting, awarding, and administering contracts.

(c) *Contractor compliance.* The agency shall establish contract surveillance programs to ensure contractors comply with the procedures established by the Defense Acquisition Regulatory Council pursuant to the preceding subsection.

(d) *Disclosing records to contractors.* Disclosing records to a contractor for use in performing a contract for the agency is considered a disclosure within the agency. The contractor is considered the agent of DCAA when receiving and maintaining the records for the agency.

§317.12 Safeguarding information in systems of records.

(a) *General responsibilities.* Appropriate administrative, technical, and physical safeguards shall be established to ensure the records in every system of records are protected from unauthorized alteration, destruction, or disclosure. The records shall be protected from reasonably anticipated