

(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.

(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 contract, the contractor activities are subject to this rule.

⁶See footnote 1 to §317.1(a).

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

(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 threats or hazards that could result in substantial harm, embarrassment, in-

convenience, or unfairness to any individual on whom information is maintained.

(b) *Minimum standards.* (1) Risk analysis and management planning shall be conducted for each system of records. Sensitivity and use of the records, present and projected threats and vulnerabilities, and present and projected cost-effectiveness of safeguards should be considered. The risk analysis may vary from an informal review of a small, relatively insensitive system to a formal, fully quantified risk analysis of a large, complex, and highly sensitive system.

(2) All personnel operating a system of records or using records from a system of records should be trained in proper record security procedures.

(3) Information exempt from disclosure under DCAA Freedom of Information Act Program (32 CFR part 290), shall be labeled to reflect its sensitivity, such as "FOR OFFICIAL USE ONLY," "PRIVACY ACT SENSITIVE: DISCLOSE ON A NEED-TO-KNOW BASIS ONLY," or some other language that alerts individuals to the sensitivity of the records.

(4) Special administrative, physical, and technical safeguards shall be employed to protect records stored or processed in an automated data processing or word processing system from threats unique to those environments.

(c) *Records disposal.* (1) Records from systems of records should be disposed of to prevent inadvertent disclosure. Disposal methods such as tearing, burning, melting, chemical decomposition, burying, pulping, pulverizing, shredding, or mutilation are considered adequate if the records are rendered unrecognizable or beyond reconstruction. Magnetic media may be cleared by degaussing, overwriting, or completely erasing.

(2) The transfer of large volumes of records (e.g., computer cards and printouts) in bulk to a disposal activity such as a Defense Reutilization and Marketing Office for authorized disposal is not a disclosure of records under this rule if volume of the records, coding of the information, or some other factor renders it impossible to recognize any personal information about a specific individual.