

(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.

(3) When disposing or destroying large quantities of records from a system of records, care must be taken to ensure that the bulk of the records is maintained to prevent easy identification of specific records. If such bulk is maintained, no special procedures are required. If bulk is not maintained, or if the form of the records makes individually identifiable information easily discernible, dispose of the records in accordance with paragraph (c)(1) of this section.

Subpart C—Collecting Information About Individuals

§ 317.20 General considerations.

(a) *Collect directly from the individual.* To the greatest extent practicable, information should be collected for systems of records directly from the individual to whom the record pertains if the record may be used to make an adverse determination about the individual's rights, benefits, or privileges under Federal programs.

(b) *Soliciting the Social Security number.* (1) It is unlawful for any Federal, State, or local government agency to deny an individual a right, benefit, or privilege provided by law because the individual refuses to provide the Social Security Number (SSN). However, this prohibition does not apply if:

(i) A Federal law requires that the SSN be provided, or

(ii) The SSN is required by a law or regulation adopted before January 1, 1975, to verify the individual's identity for a system of records established and in use before that date.

(2) Before requesting an individual to provide the SSN, the individual shall be told:

(i) Whether providing the SSN is voluntary or mandatory,

(ii) By what law or other authority the SSN is solicited, and

(iii) What uses will be made of the SSN.

(3) The notice published in the FEDERAL REGISTER for each system of records containing SSNs solicited from individuals must indicate the authority for soliciting the SSNs and whether it is mandatory for the individuals to provide their SSNs. Executive Order

9397 permits Federal agencies to solicit SSNs as numerical identifiers for individuals in Federal records systems.

(4) Upon entrance into employment with the agency, individuals must provide their SSNs; therefore, they must be given the notification. The SSN is then the individual's numerical identifier and used to establish personnel, financial, medical, and other official records. After the individual has provided the SSN to establish the records, the notification is not required when the SSN is requested only for verification or to locate the records.

(5) The Federal Personnel Manual should be consulted when soliciting SSNs for use in systems of records controlled by the Office of Personnel Management.

(c) *Collecting information about individuals from third persons.* It might not always be practical to collect all information about the individual directly from the individual, such as when:

(1) Verifying information through other sources for security or employment suitability determinations.

(2) Seeking other opinions, such as a supervisor's comments on past performance or other evaluations.

(3) Obtaining the necessary information directly from the individual will be exceptionally difficult or will result in unreasonable costs or delays; or

(4) The individual requests or consents to contacting another person to obtain the information.

(d) *Privacy Act statement.* (1) When an individual is requested to furnish information about himself or herself for a system of records, a Privacy Act statement must be provided to the individual, regardless of the method used to collect the information (forms, personal interviews, telephonic interviews, etc.). If the information requested will not be included in a system of records, a Privacy Act statement is not required.

(2) The Privacy Act statement shall include the following:

(i) The Federal law or Executive Order of the President that authorizes collecting the information.

(ii) Whether it is voluntary or mandatory for the individual to provide the requested information.