

Council, which oversees the implementation of the FAR within the Department of Defense, is responsible for developing the specific policies and procedures for soliciting, awarding, and administering contracts that are subject to this subpart and subpart G of this part and 5 U.S.C. 552a.

(3) *Contractor compliance.* Naval activities shall establish contract surveillance programs to ensure contractors comply with the procedures established by the DAR Council under the preceding subparagraph.

(4) *Disclosing records to contractors.* Disclosing records to a contractor for use in performing a contract let by a naval activity is considered a disclosure within Department of the Navy. The contractor is considered the agent of Department of the Navy when receiving and maintaining the records for that activity.

§701.106 Safeguarding records in systems of records.

Establish appropriate administrative, technical, and physical safeguards to ensure the records in every system of records are protected from unauthorized alteration, destruction, or disclosure. Protect the records from reasonably anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

(a) *Minimum standards.* (1) Conduct risk analysis and management planning for each system of records. Consider sensitivity and use of the records, present and projected threats and vulnerabilities, and present and projected cost-effectiveness of safeguards. 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) Train all personnel operating a system of records or using records from a system of records in proper record security procedures.

(3) Label information exempt from disclosure under this subpart and subpart G of this part to reflect their sensitivity, such as "FOR OFFICIAL USE ONLY," "PRIVACY ACT SENSITIVE: DISCLOSE ON A NEED-TO-KNOW

BASIS ONLY," or some other statement that alerts individuals of the sensitivity to the records.

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

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

(2) The transfer of large volumes of records (e.g., printouts and computer cards) in bulk to a disposal activity such as a Defense Reutilization and Marketing Office for authorized disposal is not a disclosure of records, if the volume of records, coding of the information, or some other factor render 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 discernable, dispose of the records in accordance with § 701.106(b)(1).

§701.107 Criteria for creating, altering, amending and deleting Privacy Act systems of records.

(a) *Criteria for a new system of records.* A new system of records is one for which no existing system notice has been published in the FEDERAL REGISTER. If a notice for a system of records has been canceled or deleted, and it is determined that it should be reinstated or reused, a new system notice must be published in the FEDERAL REGISTER. Advance public notice must