

§ 310.13

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

(iv) Maintained by a consumer reporting agency to which records have been disclosed under contract in accordance with the Federal Claims Collection Act of 1966, 31 U.S.C. 952(d).

(4) DoD Components must publish instruction that:

(i) Furnish DoD Privacy Program guidance to their personnel who solicit, award, or administer government contracts;

(ii) Inform prospective contractors of their responsibilities regarding the DoD Privacy Program; and

(iii) Establish an internal system of contractor performance review to ensure compliance with the DoD Privacy Program.

(b) *Contracting procedures.* The Defense Systems Acquisition Regulatory Council (DSARC) is responsible for developing the specific policies and procedures to be followed when soliciting bids, awarding contracts or administering contracts that are subject to this part.

(c) *Contractor compliance.* Through the various contract surveillance programs, ensure contractors comply with the procedures established in accordance with paragraph (b) above of this subpart.

(d) *Disclosure of records to contractors.* Disclosure of personal records to a contractor for the use in the performance of any DoD contract by a DoD Component is considered a disclosure within the Department of Defense (see § 310.40(b), subpart E). The contractor is considered the agent of the contracting DoD Component and to be maintaining and receiving the records for that Component.

[51 FR 2364, Jan. 16, 1986. Redesignated at 56 FR 55631, Oct. 29, 1991, and amended at 56 FR 57800, Nov. 14, 1991]

§ 310.13 Safeguarding personal information.

(a) *General responsibilities.* Establish appropriate administrative, technical and physical safeguards to ensure that the records in every system of records are protected from unauthorized alteration or disclosure and that their confidentiality is protected. Protect the records against reasonably anticipated threats or hazards that could result in substantial harm, embarrassment, in-

convenience, or unfairness to any individual about whom information is kept.

(b) *Minimum standards.* (1) Tailor system safeguards to conform to the type of records in the system, the sensitivity of the personal information stored, the storage medium used and, to a degree, the number of records maintained.

(2) Treat all unclassified records that contain personal information that normally would be withheld from the public under Exemption Numbers 6 and 7, of § 286.31, subpart D of 32 CFR part 286 (DoD Freedom of Information Act Program) as if they were designated "For Official Use Only" and safeguard them in accordance with the standards established by subpart E of 32 CFR part 286 (DoD FOIA Program) even if they are not actually marked "For Official Use Only."

(3) Afford personal information that does not meet the criteria discussed in paragraph (c)(3) of this section that degree of security which provides protection commensurate with the nature and type of information involved.

(4) Special administrative, physical, and technical procedures are required to protect data that is stored or being processed temporarily in an automated data processing (ADP) system or in a word processing activity to protect it against threats unique to those environments (see Appendices A and B).

(5) Tailor safeguards specifically to the vulnerabilities of the system.

(c) *Records disposal.* (1) Dispose of records containing personal data so as to prevent inadvertent compromise. Disposal methods such as tearing, burning, melting, chemical decomposition, pulping, pulverizing, shredding, or mutilation are considered adequate if the personal data is rendered unrecognizable or beyond reconstruction.

(2) The transfer of large quantities of records containing personal data (for example, computer cards and print-outs) in bulk to a disposal activity, such as the Defense Property Disposal Office, is not a release of personal information under this part. The sheer volume of such transfers make it difficult or impossible to identify readily specific individual records.

(3) When disposing of or destroying large quantities of records containing personal information, care must be exercised to ensure that the bulk of the records is maintained so as to prevent specific records from being readily identified. If bulk is maintained, no special procedures are required. If bulk cannot be maintained or if the form of the records make individually identifiable information easily available, dispose of the record in accordance with paragraph (c)(1) of this section.

Subpart C—Collecting Personal Information

§ 310.20 General considerations.

(a) *Collect directly from the individual.* Collect to the greatest extent practicable personal information directly from the individual to whom it pertains if the information may be used in making any determination about the rights, privileges, or benefits of the individual under any federal program (see also paragraph (c) of this section).

(b) *Collecting Social Security Numbers (SSNs).* (1) It is unlawful for any federal, state, or local governmental agency to deny an individual any right, benefit, or privilege provided by law because the individual refuses to provide his or her SSN. However, if a federal statute requires that the SSN be furnished or if the SSN is required to verify the identity of the individual in a system of records that was established and in use before January 1, 1975, and the SSN was required as an identifier by a statute or regulation adopted before that date, this restriction does not apply.

(2) When an individual is requested to provide his or her SSN, he or she must be advised:

(i) The uses that will be made of the SSN;

(ii) The statute, regulation, or rule authorizing the solicitation of the SSN; and

(iii) Whether providing the SSN is voluntary or mandatory.

(3) Include in any systems notice for any system of records that contains SSNs a statement indicating the authority for maintaining the SSN and the sources of the SSNs in the system. If the SSN is obtained directly from

the individual indicate whether this is voluntary or mandatory.

(4) Executive Order 9397, "Numbering System For Federal Accounts Relating to Individual Persons," November 30, 1943, authorizes solicitation and use of SSNs as numerical identifier for individuals in most Federal records systems. However, it does not provide *mandatory* authority for soliciting SSNs.

(5) Upon entrance into military service or civilian employment with the Department of Defense, individuals are asked to provide their SSNs. The SSN becomes the service or employment number for the individual and is used to establish personnel, financial, medical, and other official records. Provide the notification in paragraph (b)(2) of this section to the individual when originally soliciting his or her SSN. After an individual has provided his or her SSN for the purpose of establishing a record, the notification in paragraph (b)(2) is not required if the individual is only requested to furnish or verify the SSNs for identification purposes in connection with the normal use of his or her records. However, if the SSN is to be written down and retained for any purpose by the requesting official, the individual must be provided the notification required by paragraph (b)(2) of this section.

(6) Consult the Office of Personnel Management, Federal Personnel Manual (5 CFR parts 293, 294, 297 and 735) when soliciting SSNs for use in OPM records systems.

(c) *Collecting personal information from third parties.* It may not be practical to collect personal information directly from the individual in all cases. Some examples of this are:

(1) Verification of information through third party sources for security or employment suitability determinations;

(2) Seeking third party opinions such as supervisory comments as to job knowledge, duty performance, or other opinion-type evaluations;

(3) When obtaining the needed information directly from the individual is exceptionally difficult or may result in unreasonable costs; or