

130 and DoD 5400.11-R, and the Quarterly and Annual Federal Information Security Management Agency (FISMA) Privacy Reports, as required by 44 U.S.C. 3544(c), such other reports as may be required.

(xii) Update and maintain this part and DoD 5400.11-R.

Subpart B—Systems of Records

§ 310.10 General.

(a) *System of Records.* To be subject to the provisions of this part, a “system of records” must:

(1) Consist of “records” (as defined in 310.4(r)) that are retrieved by the name of an individual or some other personal identifier; and

(2) Be under the control of a DoD Component.

(b) *Retrieval practices.* (1) Records in a group of records that MAY be retrieved by a name or personal identifier are not covered by this part even if the records contain personal data and are under control of a DoD Component. The records MUST be retrieved by name or other personal identifier to become a system of records for the purpose of this part.

(i) When records are contained in an automated (Information Technology) system that is capable of being manipulated to retrieve information about an individual, this does not automatically transform the system into a system of records as defined in this part.

(ii) In determining whether an automated system is a system of records that is subject to this part, retrieval policies and practices shall be evaluated. If DoD Component policy is to retrieve personal information by the name or other unique personal identifier, it is a system of records. If DoD Component policy prohibits retrieval by name or other identifier, but the actual practice of the Component is to retrieve information by name or identifier, even if done infrequently, it is a system of records.

(2) If records are retrieved by name or personal identifier, a system notice must be submitted in accordance with § 310.33.

(3) If records are not retrieved by name or personal identifier but then are rearranged in such a manner that

they are retrieved by name or personal identifier, a new systems notice must be submitted in accordance with § 310.33.

(4) If records in a system of records are rearranged so that retrieval is no longer by name or other personal identifier, the records are no longer subject to this part and the system notice for the records shall be deleted in accordance with § 310.34.

(c) *Relevance and necessity.* Information or records about an individual shall only be maintained in a system of records that is relevant and necessary to accomplish a DoD Component purpose required by a Federal statute or an Executive Order.

(d) *Authority to establish systems of records.* Identify the specific statute or the Executive Order that authorizes maintaining personal information in each system of records. The existence of a statute or Executive Order mandating the maintenance of a system of records does not abrogate the responsibility to ensure that the information in the system of records is relevant and necessary. If a statute or Executive Order does not expressly direct the creation of a system of records, but the establishment of a system of records is necessary in order to discharge the requirements of the statute or Executive Order, the statute or Executive Order shall be cited as authority.

(e) *Exercise of First Amendment rights.*

(1) Do not maintain any records describing how an individual exercises his or her rights guaranteed by the First Amendment of the U.S. Constitution except when:

(i) Expressly authorized by Federal statute;

(ii) Expressly authorized by the individual; or

(iii) Maintenance of the information is 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.

§310.11

(f) *System Manager's evaluation.* (1) Evaluate the information to be included in each new system before establishing the system and evaluate periodically the information contained in each existing system of records for relevancy and necessity. Such a review shall also occur when a system notice alteration or amendment is prepared (see §310.33 and §310.34).

(2) Consider the following:

(i) The relationship of each item of information retained and collected to the purpose for which the system is maintained;

(ii) The specific impact on the purpose or mission of not collecting each category of information contained in the system;

(iii) The possibility of meeting the informational requirements through use of information not individually identifiable or through other techniques, such as sampling;

(iv) The length of time each item of personal information must be retained;

(v) The cost of maintaining the information; and

(vi) The necessity and relevancy of the information to the purpose for which it was collected.

(g) *Discontinued information requirements.* (1) Stop collecting immediately any category or item of personal information for which retention is no longer justified. Also delete this information from existing records, when feasible.

(2) Do not destroy any records that must be retained in accordance with disposal authorizations established under 44 U.S.C. 3303a, Examination by Archivist of Lists and Schedules of Records Lacking Preservation Value; Disposal of Records.”

§310.11 Standards of accuracy.

(a) *Accuracy of information maintained.* Maintain all personal information used or may be used to make any determination about an individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual in making any such determination.

(b) *Accuracy determinations before dissemination.* Before disseminating any personal information from a system of records to any person outside the De-

32 CFR Ch. I (7-1-12 Edition)

partment of Defense, other than a Federal Agency, make reasonable efforts to ensure the information to be disclosed is accurate, relevant, timely, and complete for the purpose it is being maintained (see §310.21(d)).

§310.12 Government contractors.

(a) *Applicability to government contractors.* (1) When a DoD Component contract requires the operation or maintenance of a system of records or a portion of a system of records or requires the performance of any activities associated with maintaining a system of records, including the collection, use, and dissemination of records, the record system or the portion of the record system affected are considered to be maintained by the DoD Component and are subject to this part. The Component is responsible for applying the requirements of this part to the contractor. The contractor and its employees are to be considered employees of the DoD Component for purposes of the criminal provisions of 5 U.S.C. 552a(i) during the performance of the contract. Consistent with the Federal Acquisition Regulation (FAR), Part 24.1, contracts requiring the maintenance or operation of a system of records or the portion of a system of records shall include in the solicitation and resulting contract such terms as are prescribed by the FAR.

(2) If the contractor must use, have access to, or disseminate individually identifiable information subject to this part in order to perform any part of a contract, and the information would have been collected, maintained, used, or disseminated by the DoD Component but for the award of the contract, these contractor activities are subject to this part.

(3) The restriction in paragraphs (a)(1) and (2) of this section do not apply to records:

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

(ii) Maintained as internal contractor employee records even when used in conjunction with providing goods and services to the Department of Defense; or

(iii) Maintained as training records by an educational organization contracted by a DoD Component to provide training when the records of the contract students are similar to and commingled with training records of other students (for example, admission forms, transcripts, academic counseling and similar records).

(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. 3711(e).

(v) Maintained by the contractor incident to normal business practices and operations.

(4) The DoD Components shall publish instructions that:

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

(ii) Inform prospective contractors of their responsibilities, and provide training as appropriate, 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 Acquisition Regulations Council shall develop 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 §310.12(b).

(d) *Disclosure of records to contractors.* Disclosure of records contained in a system of records by a DoD Component to a contractor for use in the performance of a DoD contract is considered a disclosure within the Department of Defense (see §310.21(b)). The contractor is considered the agent of the contracting DoD Component and to be maintaining and receiving the records for that Component.

§310.13 Safeguarding personal information.

(a) *General responsibilities.* DoD Components shall establish appropriate ad-

ministrative, technical and physical safeguards to ensure that the records in each system of records are protected from unauthorized access, alteration, or disclosure and that their confidentiality is preserved and protected. Records shall be protected against reasonably anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, 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 Freedom of Information Exemption Numbers 6 and 7 of 286.12, subpart C of 32 CFR part 286 ("DoD Freedom of Information Act Program") as "For Official Use Only," and safeguard them accordingly, in accordance with DoD 5200.1-R even if they are not actually marked "For Official Use Only."

(3) Personal information that does not meet the criteria discussed in paragraph (b)(2) of this section shall be accorded 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 processed in an information technology system to protect against threats unique to an automated environment (see appendix A).

(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 are those approved by the Component or the National Institute of Standards and Technology. For paper records, disposal methods, such as tearing, burning, melting, chemical decomposition, pulping, pulverizing, shredding, or mutilation are acceptable. For electronic records, and media, disposal methods, such as overwriting, degaussing, disintegration,

§ 310.14

32 CFR Ch. I (7-1-12 Edition)

pulverization, burning, melting, incineration, shredding or sanding, are acceptable.

(2) Disposal methods are considered adequate if the personal data is rendered unrecognizable or beyond reconstruction.

§ 310.14 Notification when information is lost, stolen, or compromised.

(a) If records containing personal information are lost, stolen, or compromised, the potential exists that the records may be used for unlawful purposes, such as identity theft, fraud, stalking, etc. The personal impact on the affected individual may be severe if the records are misused. To assist the individual, the Component shall promptly notify the individual of any loss, theft, or compromise (See also, § 310.50 for reporting of the breach to Senior Component Official for Privacy and the Defense Privacy Office).

(1) The notification shall be made whenever a breach occurs that involves personal information pertaining to a service member, civilian employee (appropriated or non-appropriated fund), military retiree, family member, DoD contractor, other persons that are affiliated with the Component (e.g., volunteer), and/or any other member of the public on whom information is maintained by the Component or by a contractor on behalf of the Component.

(2) The notification shall be made as soon as possible, but not later than 10 working days after the loss, theft, or compromise is discovered and the identities of the individuals ascertained.

(i) The 10 day period begins to run after the Component is able to determine the identities of the individuals whose records were lost.

(ii) If the Component is only able to identify some but not all of the affected individuals, notification shall be given to those that can be identified with follow-up notifications made to those subsequently identified.

(iii) If the Component cannot readily identify the affected individuals or will not be able to identify the individuals, the Component shall provide a generalized notice to the potentially impacted population by whatever means the Component believes is most likely to reach the affected individuals.

(3) When personal information is maintained by a DoD contractor on behalf of the Component, the contractor shall notify the Component immediately upon discovery that a loss, theft or compromise has occurred.

(i) The Component shall determine whether the Component or the contractor shall make the required notification.

(ii) If the contractor is to notify the impacted population, it shall submit the notification letters to the Component for review and approval. The Component shall coordinate with the Contractor to ensure the letters meet the requirements of § 310.14.

(4) Subject to paragraph (a)(2) of this section, the Component shall inform the Deputy Secretary of Defense of the reasons why notice was not provided to the individuals or the affected population within the 10-day period.

(i) If for good cause (e.g., law enforcement authorities request delayed notification as immediate notification will jeopardize investigative efforts), notice can be delayed, but the delay shall only be for a reasonable period of time. In determining what constitutes a reasonable period of delay, the potential harm to the individual must be weighed against the necessity for delayed notification.

(ii) The required notification shall be prepared and forwarded to the Senior Component Official for Privacy who shall forward it to the Defense Privacy Office. The Defense Privacy Office, in coordination with the Office of the Under Secretary of Defense for Personnel and Readiness, shall forward the notice to the Deputy Secretary.

(5) The notice to the individual, at a minimum, shall include the following:

(i) The individuals shall be advised of what specific data was involved. It is insufficient to simply state that personal information has been lost. Where names, social security numbers, and dates of birth are involved, it is critical that the individual be advised that these data elements potentially have been compromised.

(ii) The individual shall be informed of the facts and circumstances surrounding the loss, theft, or compromise. The description of the loss should be sufficiently detailed so that

the individual clearly understands how the compromise occurred.

(iii) The individual shall be informed of what protective actions the Component is taking or the individual can take to mitigate against potential future harm. The Component should refer the individual to the Federal Trade Commission's public Web site on identity theft at http://www.consumer.gov/idtheft/con_steps.htm. The site provides valuable information as to what steps individuals can take to protect themselves if their identities potentially have been or are stolen.

(iv) A sample notification letter is at appendix B.

(b) The notification shall be made whether or not the personal information is contained in a system of records (See § 310.10(a)).

Subpart C—Collecting Personal Information

§ 310.15 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 result in adverse determination about an individual's rights, privileges, or benefits under any Federal program.

(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 the SSN be furnished or if the SSN is furnished to a DoD Component maintaining a system of records in existence that was established and in operation before January 1, 1975, and the SSN was required under a statute or regulation adopted prior to this date for purposes of verifying the identity of an individual, this restriction does not apply.

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

(i) What uses 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.

(4) E.O. 9397, "Numbering System for Federal Accounts Relating to Individual Persons", November 30, 1943, authorizes solicitation and use of SSNs as a numerical identifier for Federal personnel that are identified in most Federal record systems. However, it does not constitute authority for mandatory disclosure of the SSN.

(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. The notification in paragraph (b)(2) of this section shall be provided the individual when originally soliciting his or her SSN. The notification is not required if an individual is requested to furnish his SSN for identification purposes and the SSN is solely used to verify the SSN that is contained in the records. However, if the SSN is solicited and retained for any purposes other than verifying the existing SSN in the records, the requesting official shall provide the individual the notification required by paragraph (b)(2) of this section.

(6) Components shall ensure that the SSN is only collected when there is a demonstrated need for collection. If collection is not essential for the purposes for which the record or records are being maintained, it should not be solicited.

(7) DoD Components shall continually review their use of the SSN to determine whether such use can be eliminated, restricted, or concealed in Component business processes, systems and paper and electronic forms. While use of the SSN may be essential for program integrity and national security when information about an individual is disclosed outside the DoD, it may not be as critical when the information is being used for internal Departmental purposes.