

## Office of the Secretary of Defense

## § 310.6

(4) To ensure that all records used in making determinations about individuals are accurate, relevant, timely, and complete.

(5) To make reasonable efforts to ensure that records containing personal information are accurate, relevant, timely, and complete for the purposes for which the record is being maintained before making them available to any recipients outside the Department of Defense, other than a federal agency, unless the disclosure is made under 32 CFR part 286.

(6) To keep no record that describes how individuals exercise their rights guaranteed by the First Amendment of the U.S. Constitution, unless expressly authorized by statute or by the individual to whom the records pertains, or the record is pertinent to and within the scope of an authorized law enforcement activity.

(7) To make reasonable efforts, when appropriate, to notify individuals whenever records pertaining to them are made available under compulsory legal process, if such process is a matter of public record.

(8) To establish safeguards to ensure the security of personal information and to protect this information from threats or hazards that might result in substantial harm, embarrassment, inconvenience, or unfairness to the individual.

(9) To establish rules of conduct for DoD personnel involved in the design, development, operation, or maintenance of any system of records and to train them in these rules of conduct.

(d) *Required public notice and publication.* DoD Components are required to publish in the FEDERAL REGISTER:

(1) A notice of the existence and character of every system of records maintained.

(2) A notice of the establishment of any new or revised system of records.

(3) At least 30 days before adoption, advance notice for public comment of any new or intended changes to the routine uses of the information in existing system of records including the categories of users and the purposes of such use.

(e) *Permit exempting eligible systems of records.* DoD Components may exempt from certain specific provisions of the

Privacy Act (5 U.S.C. 552a) eligible systems of records, but only when there is an important public purpose to be served and specific statutory for the exemption exists.

(f) *May require annual and other reports.* DoD Components shall furnish the Privacy Office that information required to complete any reports required by the Office of Management and Budget or other authorities.

### § 310.5 Organization.

(a) *Defense Privacy Board.* Membership of the board shall consist of the Executive Secretary and representatives designated by the Secretaries of the Military Departments; the Assistant Secretary of Defense (Comptroller) (whose designee shall serve as chairman); the Assistant Secretary of Defense (Force Management and Personnel); the General Counsel, Department of Defense; and the Director, Defense Logistics Agency;

(b) *The Defense Privacy Office.* The office shall consist of a Director, who shall also function as the Executive Secretary of the Defense Privacy Board, and his staff.

(c) *The Defense Privacy Board Legal Committee.* The committee shall be composed of a legal counsel from each of the DoD Components represented on the DoD Privacy Board. The legal counsels shall be appointed by the Executive Secretary in coordination with the Secretaries of the Military Department or the head of the appropriate DoD Components. Other DoD legal counsels may be appointed by the Executive Secretary, after coordination with the appropriate representative of the DoD Component concerned, to serve on the committee.

### § 310.6 Responsibilities.

(a) *The Assistant Secretary of Defense (Comptroller) (ASD(C)),* or his designee, the *Deputy Assistant Secretary of Defense (Administration) (DASD(A)),* shall:

(1) Direct and administer the DoD Privacy Program.

(2) Develop and maintain DoD Directive 5400.11 and DoD Regulation 5400.11-R (32d CFR part 310) consistent with DoD 5025.1-M and other guidance, to ensure timely and uniform implementation of the DoD Privacy Program.

### §310.6

### 32 CFR Ch. I (7–1–99 Edition)

(3) Serve as chairman of the Defense Privacy Board.

(b) *Chairman and members of the Defense Privacy Board* shall:

(1) Serve as the principal policy-makers for the DoD Privacy Program and the focal point for implementation of this part.

(2) Ensure that all DoD Components actively participate in establishing policies, procedures, and practices in carrying out the DoD Privacy Program.

(c) *Director, Defense Privacy Office*, shall:

(1) Serve as Executive Secretary and a Member of the Defense Privacy Board.

(2) Monitor implementation of the DoD Privacy Program for the Defense Privacy Board.

(3) Serve as the focal point for the coordination of Privacy Act matters with the Defense Privacy Board; the Defense Privacy Board Legal Committee; the Office of Management and Budget; the General Accounting Office; the Office of the Federal Register, in conjunction with the OSD Federal Register Liaison Officer, and other federal agencies, as required;

(4) Develop and maintain the DoD Privacy Program, DoD Directive 5400.11 and DoD 5400.11-R (32 CFR part 310) consistent with DoD 5025.1-M.

(5) Review DoD Component instructions and related issuances pertaining to the DoD Privacy Program and provide overall guidance to avoid conflict with DoD Privacy Program policy and procedures.

(6) Supervise the implementation of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 *et seq.*); DoD Directive 5400.12, "Obtaining Information from Financial Institutions" (32 CFR part 294) and any other legislation that impacts directly on individual privacy.

(7) In conjunction with the Office of the Assistant Secretary of Defense (Force Management and Personnel), the Office of the General Counsel, DoD; and other DoD Components:

(i) Ensure that training programs regarding DoD Privacy Program policies and procedures are established for all DoD personnel whose duties involve design, development, operation, and maintenance of any system of records.

(ii) Coordinate on all DoD personnel policies that may affect the DoD Privacy Program.

(8) In conjunction with the Office of the Deputy Assistant Secretary of Defense (Management Systems), Office of the ASD(C), and other DoD Components, ensure that:

(i) All information requirements developed to collect or maintain personal data conform with DoD Privacy Program standards;

(ii) Procedures are developed to protect personal information while it is being processed or stored in automated data processing or word processing centers.

(9) In conjunction with the Office of the ASD (FM&P), the Defense Manpower Data Center (Defense Logistics Agency), and other DoD Components, ensure that procedures developed to collect or maintain personal data for research purposes conform both to the requirements of the research and DoD Privacy Program standards.

(d) *Members of Defense Privacy Board Legal Committee* shall:

(1) Consider legal questions referred to it by the Board regarding the application of the Privacy Act (5 U.S.C. 552a); DoD Directive 5400.11; and DoD 5400.11-R, (this part) and the implementation of the DoD Privacy Program.

(2) Render advisory opinions to the DoD Privacy Board, subject to approval by the General Counsel, Department of Defense.

(e) *The General Counsel, Department of Defense*, shall:

(1) Review the advisory opinions of the Defense Privacy Board Legal Committee to ensure uniformity in legal positions and interpretations rendered.

(2) Be the final approving authority on all advisory legal opinions rendered by the Defense Privacy Board or the Defense Privacy Board Legal Committee regarding the Privacy Act (5 U.S.C. 552a) or its implementation.

(f) *The Head of each DoD Component* shall implement the DoD Privacy Program by carrying out the specific responsibilities set forth in §310.4(c) and shall:

(1) Establish an active program to implement the DoD Privacy Program.

(2) Provide adequate funds and personnel to support the Privacy Program.

(3) Designate a senior official to serve as the principal point of contact for DoD Privacy matters and to monitor compliance with the program.

(4) Ensure that DoD Privacy Program compliance is reviewed during the internal inspections conducted by Inspectors General or equivalent inspectors.

(5) Ensure that the DoD Component head, a designee, or an appellant reviews all appeals from denials or refusals by Component officials to amend personal records.

(6) Establish rules of conduct to ensure that:

(i) Only personal information that is relevant and necessary to achieve a purpose required by statute or Executive Order is collected, maintained, used or disseminated.

(ii) Personal information is collected to the greatest extent practicable directly from the individual to whom it pertains.

(iii) No records are maintained describing how individuals exercise their rights guaranteed by the First Amendment to the U.S. Constitution unless expressly authorized by statute or the individual to whom they pertain or unless the records pertain to and are within the scope of an authorized law enforcement activity.

(iv) Individuals are granted access to records which pertain to them in systems of records unless the system has been exempted from the access provisions of the Privacy Act (5 U.S.C. 552a).

(v) No system of records subject to the Privacy Act (5 U.S.C. 552a) is maintained, used, or disseminated without prior publication of a system notice in the FEDERAL REGISTER.

(vi) All personal information contained in any system of records is safeguarded against unwarranted and unauthorized disclosure.

(vii) Procedures are established that permit an individual to seek the correction or amendment of any record in a system of records pertaining to the individual unless system of records has been exempted from the amendment procedures of the Privacy Act (5 U.S.C. 552a).

(viii) All personnel whose duties involve design, development, operation, and maintenance of any system of records are trained in the rules of conduct established.

(ix) Assist, upon request, the Defense Privacy Board on matters of special interest.

(g) The *System Manager* for any system of records shall:

(1) Ensure that all personnel who either have access to the system of record or who are engaged in developing or supervising procedures for handling records in the system of records in the system of records are aware of their responsibilities for protecting personal information established by the DoD Privacy Program.

(2) Prepare promptly any required new, amended, or altered system notices for the system of records and submit them through channels for publication in the FEDERAL REGISTER.

(3) Notify all Automated Data Processing (ADP) or word processing managers who process information from the system of records that the information is subject to the DoD Privacy Program and the applicable routine uses for the information in the system.

(4) Coordinate with ADP and word processing managers providing services to ensure an adequate risk analysis is conducted.

(5) Coordinate with the servicing ADP and word processing managers to ensure that the system manager is notified when there are changes to processing equipment, hardware or software, and the data base that may require submission of an amended system notice.

(h) *Automated Data Processing (ADP) or Word Processing Managers*, who process information from any system of records, shall:

(1) Ensure that each system manager provides a current system notice or information as to the contents of the system notice for each system of records from which information is to be processed.

(2) Ensure that all personnel who have access to information from a system of records during processing or who are engaged in developing procedures for processing such information are aware of the provisions of the DoD

## § 310.10

Privacy Program policies and procedures.

(3) Notify promptly the system manager whenever there are changes to processing equipment, hardware or software, and the data base that may require the submission of an amended system notice for any system of records.

(i) *DoD employees* shall:

(1) Not disclose any personal information contained in any system of records except as authorized in this part.

(2) Not maintain any official files which are retrievable by name or other personal identifier without first ensuring that a notice for the system has been published in the FEDERAL REGISTER.

(3) Report any disclosures of personal information from a system of records or the maintenance of any system of records that are not authorized by this part to the appropriate Privacy Act officials for his or her action.

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

### 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 § 310.3(n)) 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*, in fact, retrieved by name or other personal identifier to become a system of records for the purpose of this part.

(2) If files that are not retrieved by name or personal identifier are rearranged in such manner that they are retrieved by name or personal identifier, a new systems notice must be submitted in accordance with § 310.63(c) of subpart G.

## 32 CFR Ch. I (7–1–99 Edition)

(3) 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 § 310.64(c) of subpart G.

(c) *Relevance and necessity.* Retain in a system of records only that personal information which is relevant and necessary to accomplish a 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 authorize 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.

(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.

(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 amendment or alteration is prepared (see §§ 310.63 and 310.64 of subpart G).

(2) Consider the following:

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