

(2) When expressly authorized by the individual on whom the record is maintained; or

(3) When the record is pertinent to and within the scope of an authorized law enforcement activity.

(d) Notices shall be published in the FEDERAL REGISTER and reports shall be submitted to Congress and the Office of Management and Budget, in accordance with, and as required by, 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R, as to the existence and character of any system of records being established or revised by the DoD Components. Information shall not be collected, maintained, used, or disseminated until the required publication and review requirements, as set forth in 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R, are satisfied.

(e) Individuals shall be permitted, to the extent authorized by 5 U.S.C. 552a and DoD 5400.11-R, to:

(1) Determine what records pertaining to them are contained in a system of records.

(2) Gain access to such records and obtain a copy of those records or a part thereof.

(3) Correct or amend such records once it has been determined that the records are not accurate, relevant, timely, or complete.

(4) Appeal a denial of access or a request for amendment.

(f) Disclosure of records pertaining to an individual from a system of records shall be prohibited except with the consent of the individual or as otherwise authorized by 5 U.S.C. 552a, DoD 5400.11-R, and DoD 5400.7-R. When disclosures are made, the individual shall be permitted, to the extent authorized by references 5 U.S.C. 552a and/or DoD 5400.11-R, to seek an accounting of such disclosures from the DoD Component making the release.

(g) Disclosure of records pertaining to personnel of the National Security Agency, the Defense Intelligence Agency, the National Reconnaissance Office, and the National Geospatial-Intelligence Agency shall be prohibited to the extent authorized by Public Law 86-36 (1959) and 10 U.S.C. 424. Disclosure of records pertaining to personnel of overseas, sensitive, or routinely deployable units shall be prohibited to

the extent authorized by 10 U.S.C. 130b. Disclosure of medical records is prohibited except as authorized by DoD 6025.18-R.⁶

(h) Computer matching programs between the DoD Components and the Federal, State, or local governmental agencies shall be conducted in accordance with the requirements of 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R.

(i) DoD personnel and system managers shall conduct themselves consistent with established rules of conduct 310.8 so that personal information to be stored in a system of records only shall be collected, maintained, used, and disseminated as is authorized by this part, 5 U.S.C. 552a and DoD 5400.11-R.

(j) DoD personnel, including but not limited to family members, retirees, contractor employees, and volunteers, shall be notified, in a timely manner, consistent with the requirements of DoD 5400.11-R, if their personal information, whether or not included in a system of records, is lost, stolen, or compromised.

(k) DoD Field Activities shall receive Privacy Program support from the Director, Washington Headquarters Services.

§ 310.6 Responsibilities.

(a) The Director of Administration and Management, Office of the Secretary of Defense, shall:

(1) Serve as the Senior Privacy Official for the Department of Defense.

(2) Provide policy guidance for, and coordinate and oversee administration of, the DoD Privacy Program to ensure compliance with policies and procedures in 5 U.S.C. 552a and OMB Circular A-130.

(3) Publish DoD 5400.11-R and other guidance, including Defense Privacy Board Advisory Opinions, to ensure timely and uniform implementation of the DoD Privacy Program.

(4) Serve as the Chair to the Defense Privacy Board and the Defense Data Integrity Board (see § 310.9).

(5) Supervise and oversee the activities of the Defense Privacy Office (see § 310.9).

⁶See footnote 1 to § 310.1.

§310.7

(b) The Director, WHS, under the DA&M, shall provide Privacy Program support for DoD Field Activities.

(c) The General Counsel of the Department of Defense shall:

(1) Provide advice and assistance on all legal matters arising out of, or incident to, the administration of the DoD Privacy Program.

(2) Review and be the final approval authority on all advisory opinions issued by the Defense Privacy Board or the Defense Privacy Board Legal Committee.

(3) Serve as a member of the Defense Privacy Board, the Defense Data Integrity Board, and the Defense Privacy Board Legal Committee (310.9).

(d) The Secretaries of the Military Departments and the Heads of the Other DoD Components, except as noted in §310.5(k), shall:

(1) Provide adequate funding and personnel to establish and support an effective DoD Privacy Program, to include the appointment of a senior official to serve as the principal point of contact (POC) for DoD Privacy Program matters.

(2) Establish procedures, as well as rules of conduct, necessary to implement this part and DoD 5400.11-R to ensure compliance with the requirements of 5 U.S.C. 552a and OMB Circular A-130.

(3) Conduct training, consistent with the requirements of DoD 5400.11-R, on the provisions of this part, 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R, for assigned, employed and detailed, to include contractor, personnel and individuals having primary responsibility for implementing the DoD Privacy Program.

(4) Ensure all Component legislative proposals, policies, or programs having privacy implications, such as the DoD Privacy Impact Assessment Program, are evaluated to ensure consistency with the information privacy principles of this part and DoD 5400.11-R.

(5) Assess the impact of technology on the privacy of personal information and, when feasible, adopt privacy-enhancing technology both to preserve and protect personal information contained in Component systems of records and to permit auditing of com-

32 CFR Ch. I (7-1-10 Edition)

pliance with the requirements of this part and DoD 5400.11-R.

(6) Ensure the DoD Privacy Program periodically shall be reviewed by the Inspectors General or other officials, who shall have specialized knowledge of the DoD Privacy Program.

(7) Submit reports, consistent with the requirements of DoD 5400.11-R, as mandated by 5 U.S.C. 552a and OMB Circular A-130, and DoD Directive 5500.1, and as otherwise directed by the DPO.

(e) The Secretaries of the Military Departments shall provide support to the Combatant Commands, as identified in DoD Directive 5100.3,⁷ in the administration of the DoD Privacy Program.

§310.7 Information requirements.

The reporting requirements in §310.6(d)(7) are assigned Report Control Symbol DD-DA&M(A)1379.

§310.8 Rules of conduct.

(a) DoD personnel shall:

(1) Take such actions, as considered appropriate, to ensure that personal information contained in a system of records, to which they have access to or are using incident to the conduct of official business, shall be protected so that the security and confidentiality of the information shall be preserved.

(2) Not disclose any personal information contained in any system of records except as authorized by DoD 5400.11-R or other applicable law or regulation. Personnel willfully making such a disclosure when knowing that disclosure is prohibited are subject to possible criminal penalties and/or administrative sanctions.

(3) Report any unauthorized 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 applicable Privacy POC for his or her DoD Component.

(b) DoD System Managers for each system of records shall:

(1) Ensure that all personnel who either shall have access to the system of records or who shall develop or supervise procedures for handling records in

⁷ See footnote 1 to §310.1.