

§ 316.7

unauthorized or unintentional access, disclosure, modification or destruction and to insure that all persons whose official duties require access to or processing and maintenance of personal information are trained in the proper safeguarding and use of such information.

[40 FR 55535, Nov. 28, 1975. Redesignated and amended at 57 FR 6074, Feb. 20, 1992; 62 FR 26389, May 14, 1997]

§ 316.7 Questions.

Questions on both the substance and procedure of the Privacy Act and the DISA implementation thereof should be addressed to the DISA Counsel by the most expeditious means possible, including telephone calls.

[40 FR 55535, Nov. 28, 1975. Redesignated at 57 FR 6074, Feb. 20, 1992, as amended at 62 FR 26390, May 14, 1997]

§ 316.8 Exemptions.

Section 5 U.S.C. 552a (3)(j) and (3)(k) authorize an agency head to exempt certain systems of records or parts of certain systems of records from some of the requirements of the act. This part reserves to the Director, DISA, as head of an agency, the right to create exemptions pursuant to the exemption provisions of the act. All systems of records maintained by DISA shall be exempt from the requirements of 5 U.S.C. 552a (d) pursuant to 5 U.S.C. 552a(3)(k)(1) to the extent that the system contains any information properly classified under Executive Order 11652, "Classification and Declassification of National Security Information and Material," dated March 8, 1972 (37 FR 10053, May 19, 1972) and which is required by the executive order to be kept secret in the interest of national defense or foreign policy. This exemption, which may be applicable to parts of all systems of records, is necessary because certain record systems not otherwise specifically designated for exemptions may contain isolated information which has been properly classified.

[42 FR 20298, Apr. 19, 1977. Redesignated at 57 FR 6074, Feb. 20, 1992, as amended at 62 FR 26390, May 14, 1997]

32 CFR Ch. I (7-1-03 Edition)

PART 317—DCAA PRIVACY ACT PROGRAM

Sec.

- 317.1 Purpose.
- 317.2 Applicability and scope.
- 317.3 Policy.
- 317.4 Responsibilities.
- 317.5 Information requirements.
- 317.6 Procedures.

AUTHORITY: Pub. L. 93-579, 88 Stat. 1896 (5 U.S.C. 552a).

SOURCE: 65 FR 63799, Oct. 25, 2000, unless otherwise noted.

§ 317.1 Purpose

This part provides policies and procedures for the Defense Contract Audit Agency's implementation of the Privacy Act of 1974 (DCAA Regulation 5410.10,¹ as amended, (5 U.S.C. 552a); DoD 5400.11 and DoD 5400.11-R,² "DoD Privacy Program" (32 CFR part 310); and is intended to promote uniformity within DCAA.

§ 317.2 Applicability and scope.

(a) This part applies to all DCAA organizational elements and takes precedence over all regional regulatory issuances that supplement the DCAA Privacy Program.

(b) This part shall be made applicable by contract or other legally binding action to contractors whenever a DCAA contract provides for the operation of a system of records or portion of a system of records to accomplish an Agency function.

§ 317.3 Policy.

(a) It is DCAA policy that personnel will comply with the DCAA Privacy Program; the Privacy Act of 1974; and the DoD Privacy Program (32 CFR part 310). Strict adherence is necessary to ensure uniformity in the implementation of the DCAA Privacy Program and create conditions that will foster public trust. It is also Agency policy to safeguard personal information contained in any system of records maintained by DCAA organizational elements and to make that information

¹Copies may be obtained from <http://www.deskbook.osd.mil>.

²Copies may be obtained from <http://web7.whs.osd.mil>.

available to the individual to whom it pertains to the maximum extent practicable.

(b) DCAA policy specifically requires that DCAA organizational elements:

(1) Collect, maintain, use, and disseminate personal information only when it is relevant and necessary to achieve a purpose required by statute or Executive Order.

(2) Collect personal information directly from the individuals to whom it pertains to the greatest extent practical.

(3) Inform individuals who are asked to supply personal information for inclusion in any system of records:

(i) The authority for the solicitation.

(ii) Whether furnishing the information is mandatory or voluntary.

(iii) The intended uses of the information.

(iv) The routine disclosures of the information that may be made outside of DoD.

(v) The effect on the individual of not providing all or any part of the requested information.

(4) Ensure that records used in making determinations about individuals and those containing personal information are accurate, relevant, timely, and complete for the purposes for which they are being maintained before making them available to any recipients outside of DoD, other than a Federal agency, unless the disclosure is made under DCAA Regulation 5410.8, DCAA Freedom of Information Act Program.³

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

(6) Notify individuals whenever records pertaining to them are made available under compulsory legal processes, if such process is a matter of public record.

(7) Establish safeguards to ensure the security of personal information and to protect this information from threats or hazards that might result in sub-

stantial harm, embarrassment, inconvenience, or unfairness to the individual.

(8) Establish rules of conduct for DCAA personnel involved in the design, development, operation, or maintenance of any system of records and train them in these rules of conduct.

(9) Assist individuals in determining what records pertaining to them are being collected, maintained, used, or disseminated.

(10) Permit individual access to the information pertaining to them maintained in any system of records, and to correct or amend that information, unless an exemption for the system has been properly established for an important public purpose.

(11) Provide, on request, an accounting of all disclosures of the information pertaining to them except when disclosures are made:

(i) To DoD personnel in the course of their official duties.

(ii) Under DCAA Regulation 5410.8, DCAA Freedom of Information Act Program.

(iii) To another agency or to an instrumentality of any governmental jurisdiction within or under control of the United States conducting law enforcement activities authorized by law.

(12) Advise individuals on their rights to appeal any refusal to grant access to or amend any record pertaining to them, and file a statement of disagreement with the record in the event amendment is refused.

§317.4 Responsibilities.

(a) The Assistant Director, Resources has overall responsibility for the DCAA Privacy Act Program and will serve as the sole appellate authority for appeals to decisions of respective initial denial authorities.

(b) The Chief, Administrative Management Division under the direction of the Assistant Director, Resources, shall:

(1) Establish, issue, and update policies for the DCAA Privacy Act Program; monitor compliance with this part; and provide policy guidance for the DCAA Privacy Act Program.

(2) Resolve conflicts that may arise regarding implementation of DCAA Privacy Act policy.

³Copies may be obtained from <http://www.deskbook.osd.mil>.

§ 317.4

32 CFR Ch. I (7–1–03 Edition)

(3) Designate an Agency Privacy Act Advisor, as a single point of contact, to coordinate on matters concerning Privacy Act policy.

(4) Make the initial determination to deny an individual's written Privacy Act request for access to or amendment of documents filed in Privacy Act systems of records. This authority cannot be delegated.

(c) The DCAA Privacy Act Advisor under the supervision of the Chief, Administrative Management Division shall:

(1) Manage the DCAA Privacy Act Program in accordance with this part and applicable DCAA policies, as well as DoD and Federal regulations.

(2) Provide guidelines for managing, administering, and implementing the DCAA Privacy Act Program.

(3) Implement and administer the Privacy Act program at the Headquarters.

(4) Ensure that the collection, maintenance, use, or dissemination of records of identifiable personal information is in a manner that assures that such action is for a necessary and lawful purpose; that the information is timely and accurate for its intended use; and that adequate safeguards are provided to prevent misuse of such information.

(5) Maintain and publish DCAA Pamphlet 5410.13, DCAA Compilation of Privacy Act System Notices.⁴

(6) Prepare promptly any required new, amended, or altered system notices for systems of records subject to the Privacy Act and submit them to the Defense Privacy Office for subsequent publication in the FEDERAL REGISTER.

(7) Prepare the annual Privacy Act Report as required by DoD 5400.11–5, DoD Privacy program.

(8) Conduct training on the Privacy Act program for Agency personnel.

(d) Heads of Principal Staff Elements are responsible for:

(1) Reviewing all regulations or other policy and guidance issuances for

which they are the proponent to ensure consistency with the provisions of this part.

(2) Ensuring that the provisions of this part are followed in processing requests for records.

(3) Forwarding to the DCAA Privacy Act Advisor, any Privacy Act requests received directly from a member of the public, so that the request may be administratively controlled and processed.

(4) Ensuring the prompt review of all Privacy Act requests, and when required, coordinating those requests with other organizational elements.

(5) Providing recommendations to the DCAA Privacy Act Advisor regarding the releasability of DCAA records to members of the public, along with the responsive documents.

(6) Providing the appropriate documents, along with a written justification for any denial, in whole or in part, of a request for records to the DCAA Privacy Act Advisor. Those portions to be excised should be bracketed in red pencil, and the specific exemption or exemptions cites which provide the basis for denying the requested records.

(e) The General Counsel is responsible for:

(1) Ensuring uniformity is maintained in the legal position, and the interpretation of the Privacy Act; 32 CFR part 310; and this part.

(2) Consulting with DoD General Counsel on final denials that are inconsistent with decisions of other DoD components, involve issues not previously resolved, or raise new or significant legal issues of potential significance to other Government agencies.

(3) Providing advice and assistance to the Assistant Director, Resources; Regional Directors; and the Regional Privacy Act Officer, through the DCAA Privacy Act Advisor, as required, in the discharge of their responsibilities.

(4) Coordinating Privacy Act litigation with the Department of Justice.

(5) Coordinating on Headquarters denials of initial requests.

(f) Each Regional Director is responsible for the overall management of the Privacy Act program within their respective regions. Under his/her direction, the Regional Resources Manager

⁴Copies may be obtained from the Defense Contract Audit Agency, ATTN: DCAA-CMO, 8725 John J. Kingman Road, Suite 2135, Fort Belvoir, VA 22060–6219. Electronic copies of DCAA Privacy notices may be obtained from <http://www.defenselink.mil/privacy>.

is responsible for the management and staff supervision of the program and for designating a Regional Privacy Act Officer. Regional Directors will, as designee of the Director, make the initial determination to deny an individual's written Privacy Act request for access to or amendment of documents filed in Privacy Act systems of records. This authority cannot be delegated.

(g) Regional Privacy Act Officers will:

(1) Implement and administer the Privacy Act program throughout the region.

(2) Ensure that the collection, maintenance, use, or dissemination of records of identifiable personal information is in a DCAAR 5410.10 manner that assures that such action is for a necessary and lawful purpose; that the information is timely and accurate for its intended use; and that adequate safeguards are provided to prevent misuse of such information.

(3) Prepare input for the annual Privacy Act Report when requested by the DCAA Information and Privacy Advisor.

(4) Conduct training on the Privacy Act program for regional and FAO personnel.

(5) Provide recommendations to the Regional Director through the Regional Resources Manager regarding the releasability of DCAA records to members of the public.

(h) Managers, Field Audit Offices (FAOs) will:

(1) Ensure that the provisions of this part are followed in processing requests for records.

(2) Forward to the Regional Privacy Act Officer, any Privacy Act requests received directly from a member of the public, so that the request may be administratively controlled and processed.

(3) Ensure the prompt review of all Privacy Act requests, and when required, coordinating those requests with other organizational elements.

(4) Provide recommendation to the Regional Privacy Act Officer regarding the releasability of DCAA records to members of the public, along with the responsive documents.

(5) Provide the appropriate documents, along with a written justifica-

tion for any denial, in whole or in part, of a request for records to the Regional Privacy Act Officer. Those portions to be excised should be bracketed in red pencil, and the specific exemption or exemptions cited which provide the basis for denying the requested records.

(i) DCAA Employees will:

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

(2) Not maintain any official files which are retrieved 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 their action.

§317.5 Information requirements.

The Report Control Symbol. Unless otherwise directed, any report concerning implementation of the Privacy Program shall be assigned Report Control Symbol DD-DA&M(A)1379.

§317.6 Procedures.

Procedures for processing material in accordance with the Privacy Act of 1974 are outlined in DoD 5400.11-R, DoD Privacy Program (32 CFR part 310).

PART 318—DEFENSE THREAT REDUCTION AGENCY PRIVACY PROGRAM

Sec.

318.1 Reissuance and purpose.

318.2 Application.

318.3 Definitions.

318.4 Policy.

318.5 Designations and responsibilities.

318.6 Procedures for requests pertaining to individual records in a record system.

318.7 Disclosure of requested information to individuals.

318.8 Request for correction or amendment to a record.

318.9 Agency review of request for correction or amendment of record.

318.10 Appeal of initial adverse Agency determination for access, correction or amendment.

318.11 Disclosure of record to persons other than the individual to whom it pertains.