§ 317.5 Information requirements.

The Report Control Symbol. Unless otherwise directed, any report concerning implementation of the Privacy Act program for regional and FAO personnel.

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

(5) Provide recommendations to the Regional Privacy Act Officer 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 recommendations 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 justification 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 Act program for regional and FAO personnel.

(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 recommendations 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 justification 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.
§ 318.1 Reissuance and purpose.

(a) This part updates the policies, responsibilities, and procedures of the DTRA Privacy Program under the Privacy Act of 1974, as amended (5 U.S.C. 552a), OMB Circular A-130,1 and the DoD Privacy Program (32 CFR part 310).

(b) This rule establishes procedures whereby individuals can:

(1) Request notification of whether Defense Threat Reduction Agency (DTRA) maintains or has disclosed a record pertaining to them in any non-exempt system of records;

(2) Request a copy or other access to such a record or to an accounting of its disclosure;

(3) Request that the record be amended; and

(4) Appeal any initial adverse determination of any such request.

(c) Specifies those system of records which the Director, Defense Threat Reduction Agency has determined to be exempt from the procedures established by this rule and by certain provisions of the Privacy Act.

(d) DTRA policy encompasses the safeguarding of individual privacy from any misuse of DTRA records and the provides the fullest access practicable by individuals to DTRA records concerning them.

§ 318.2 Applicability.

(a) This part applies to all members of the Armed Forces and Department of Defense civilians assigned to the DTRA at any of its duty locations.

(b) This part shall be made applicable to DoD contractors who are operating a system of records on behalf of DTRA, to include any of the activities, such as collecting and disseminating records, associated with maintaining a system of records.

§ 318.3 Definitions.

Access. The review of a record or a copy of a record or parts thereof in a system of records by any individual.

Agency. For the purposes of disclosing records subject to the Privacy Act among DoD Components, the Department of Defense is considered a single agency. For all other purposes to include applications for access and amendment, denial of access or amendment, appeals from denials, and record keeping as regards release to non-DoD agencies; each DoD Component is considered an agency within the meaning of the Privacy Act.

Confidential source. A person or organization who has furnished information to the federal government under an express promise that the person's or the organization's identity will be held in confidence or under an implied promise of such confidentiality if this implied promise was made before September 27, 1975.