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 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 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.

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

SOURCE: 65 FR 18894, Apr. 10, 2000, unless otherwise noted.

§ 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 nonexempt 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.

Disclosure. The transfer of any personal information from a system of records by any means of communication (such as oral, written, electronic, mechanical, or actual review) to any person, private entity, or government agency, other than the subject of the record, the subject's designated agent or the subject's legal guardian.

Individual. A living person who is a citizen of the United States or an alien lawfully admitted for permanent residence. The parent of a minor or the legal guardian of any individual also may act on behalf of an individual. Corporations, partnerships, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities are not ''individuals.''

Law enforcement activity. Any activity engaged in the enforcement of criminal laws, including efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities.

Maintain. Includes maintain, collect, use or disseminate.

[1] Copies may be obtained: http://www.whitehouse.gov/OMB/circulars.

Official use. Within the context of this part, this term is used when officials and employees of a DoD Component have a demonstrated need for the use of any record or the information contained therein in the performance of their official duties, subject to DoD 5200.1–R,[2] ''DoD Information Security Program Regulation''.

Personal information. Information about an individual that identifies, relates or is unique to, or describes him or her; e.g., a social security number, age, military rank, civilian grade, marital status, race, salary, home/office phone numbers, etc.

Privacy Act request. A request from an individual for notification as to the existence of, access to, or amendment of records pertaining to that individual. These records must be maintained in a system of records.

Member of the public. Any individual or party acting in a private capacity to include federal employees or military personnel.

Record. Any item, collection, or grouping of information, whatever the storage media (e.g., paper, electronic, etc.), about an individual that is maintained by a DoD Component, including but not limited to, his or her education, financial transactions, medical history, criminal or employment history and that contains his or her name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

Risk assessment. An analysis considering information sensitivity, vulnerabilities, and the cost to a computer facility or word processing activity in safeguarding personal information processed or stored in the facility or activity.

Routine use. The disclosure of a record outside the Department of Defense for a use that is compatible with the purpose for which the information was collected and maintained by the Department of Defense. The routine use must be included in the published system notice for the system of records involved.

[2]Copies may be obtained: http://web7.whs.osd.mil/corres.htm.

Statistical record. A record maintained only for statistical research or reporting purposes and not used in whole or in part in making determinations about specific individuals.

System manager. The DoD Component official who is responsible for the operation and management of a system of records.

System of records. A group of records under the control of a DoD Component from which personal information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to an individual.

Word processing system. A combination of equipment employing automated technology, systematic procedures, and trained personnel for the primary purpose of manipulating human thoughts and verbal or written or graphic presentations intended to communicate verbally or visually with another individual.

Word processing equipment. Any combination of electronic hardware and computer software integrated in a variety of forms (firmware, programmable software, handwiring, or similar equipment) that permits the processing of textual data. Generally, the equipment contains a device to receive information, a computer-like processor with various capabilities to manipulate the information, a storage medium, and an output device

§318.4 Policy.

(a) It is DTRA policy that:

(1) The personal privacy of an individual shall be respected and protected. Personal information shall be collected, maintained, used, or disclosed to insure that:

(2) It shall be relevant and necessary to accomplish a lawful DTRA purpose required to be accomplished by Federal statute or Executive order;

(3) It shall be collected to the greatest extent practicable directly from the individual;

(4) The individual shall be informed as to why the information is being collected, the authority for collection, what uses will be made of it, whether disclosure is mandatory or voluntary, and the consequences of not providing the information;

(5) It shall be relevant, timely, complete and accurate for its intended use; and

(6) Appropriate administrative, technical, and physical safeguards shall be established, based on the media (e.g., paper, electronic, etc.) involved, to ensure the security of the records and to prevent compromise or misuse during storage or transfer.

(b) No record shall be maintained on how an individual exercises rights guaranteed by the First Amendment to the Constitution, except as specifically authorized by statute; expressly authorized by the individual on whom the record is maintained; or when the record is pertinent to and within the scope of an authorized law enforcement activity.

(c) 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 32 CFR part 310, 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, or disseminated until the required publication/review requirements are satisfied.

(d) Individuals shall be permitted, to the extent authorized by this part:

(1) To 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 on a showing the records are not accurate, relevant, timely, or complete.

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

(e) 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 and 32 CFR part 286. When disclosures are made, the individual shall be permitted, to the extent authorized by 5 U.S.C. 552a and 32 CFR part 310, to seek an accounting of such disclosures from DTRA.

(f) Computer matching programs between DTRA and 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 32 CFR part 310.

(g) DTRA personnel and Systems Managers shall conduct themselves, pursuant to established rules of conduct, so that personal information to be stored in a system of records shall only be collected, maintained, used, and disseminated as authorized by this part.

§ 318.5 Designations and responsibilities

(a) The Director, DTRA shall:

(1) Provide adequate funding and personnel to establish and support an effective Privacy Program.

(2) Appoint a senior official to serve as the Agency Privacy Act Officer.

(3) Serve as the Agency Appellate Authority.

(b) The Privacy Act Officer shall:

(1) Implement the Agency's Privacy Program in accordance with the specific requirements set forth in this part, 5 U.S.C. 552a, OMB Circular A–130, and 32 CFR part 310.

(2) Establish procedures, as well as rules of conduct, necessary to implement this part so as to ensure compliance with the requirements of 5 U.S.C. 552a, OMB Circular A–130, and 32 CFR part 310.

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

(4) Serve as the Agency Initial Denial Authority.

(c) *The Privacy Act Program Manager shall:*

(1) Manage activities in support of the DTRA Program oversight in accordance with part, 5 U.S.C. 552a, OMB Circular A–130, and 32 CFR part 310.

(2) Provide operational support, guidance and assistance to Systems Managers for responding to requests for access/amendment of records.

(3) Direct the day-by-day activities of the DTRA Privacy Program.

(4) Provide guidance and assistance to DTRA elements in their implementation and execution of the DTRA Privacy Program.

(5) Prepare and submit proposed new, altered, and amended systems of records, to include submission of required notices for publication in the Federal Register consistent with this part, 5 U.S.C. 552a, OMB Circular A–130, and 32 CFR part 310.

(6) Prepare and submit proposed DTRA privacy rulemaking, to include documentation for submission of the proposed rule to the Office of the Federal Register for publication. Additionally, provide required documentation for reporting to the OMB and Congress, consistent with this part, 5 U.S.C. 552a, OMB Circular A–130, and 32 CFR part 310.

(7) Provide advice and support to DTRA elements to ensure that:

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

(ii) Appropriate procedures and safeguards shall be developed, implemented, and maintained to protect personal information when it is stored in either a manual and/or automated system of records or transferred by electronic or non-electronic means; and

(iii) Specific procedures and safeguards shall be developed and implemented when personal data is collected and maintained for research purposes.

(8) Conduct reviews, and prepare and submit reports consistent with the requirements in this part, 5 U.S.C. 552a, OMB Circular A–130, and 32 CFR part 310, or as otherwise directed by the Defense Privacy Office.

(9) Conduct training for all assigned and employed DTRA personnel and for those individuals having primary responsibility for DTRA Privacy Act Record Systems consistent with requirements of this part, 5 U.S.C. 552a, OMB Circular A–130, and 32 CFR part 310.

(10) Serve as the principal points of contact for coordination of privacy and related matters.

(d) *The Directorate Heads and Office Chiefs shall:*

(1) Recognize and support the DTRA Privacy Act Program.

(2) Appoint an individual to serve as Privacy Act Point of Contact within their purview.

(3) Initiate prompt, constructive management actions on agreed-upon actions identified in agency Privacy Act reports.

(e) *The Chief, Information Systems shall:*

(1) Ensure that all personnel who have access to information from an automated system of records during processing or who are engaged in developing procedures for processing such information are aware of the provisions of this Instruction.

(2) Promptly notify automated system managers and the Privacy Act Officer whenever they are changes to Agency Information Technology that may require the submission of an amended system notice for any system of records.

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

(f) Agency System Managers shall exercise the Rules of Conduct as specified in 32 CFR part 310.

(g) Agency personnel shall exercise the Rules of Conduct as specified in 32 CFR part 310.

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

(a) An individual seeking notification of whether a system of records, maintained by the Defense Threat Reduction Agency, contains a record pertaining to himself/herself and who desires to review, have copies made of such records, or to be provided an accounting of disclosures from such records, shall submit his or her request in writing. Requesters are encourage to review the systems of records notices published by the Agency so as to specifically identify the particular record system(s) of interest to be accessed.

(b) In addition to meeting the requirements set forth in this section 318.6, the individual seeking notification, review or copies, and an accounting of disclosures will provide in writing his or her full name, address, Social Security Number, and a telephone number where the requester can be

contacted should questions arise concerning the request. This information will be used only for the purpose of identifying relevant records in response to an individual's inquiry. It is further recommended that individuals indicate any present or past relationship or affiliations, if any, with the Agency and the appropriate dates in order to facilitate a more thorough search. A notarized statement or an unsworn declaration in accordance with 28 U.S.C. 1746 may also be required.

(c) An individual who wishes to be accompanied by another individual when reviewing his or her records, must provide the Agency with written consent authorizing the Agency to disclose or discuss such records in the presence of the accompanying individual.

(d) Individuals should mail their written request to the FOIA/Privacy Act Division, Defense Threat Reduction Agency, 45045 Aviation Drive, Dulles, VA 20166–7517 and indicate clearly on the outer envelope ''Privacy Act Request.''

§ 318.7 Disclosure of requested information to individuals.

(a) The Defense Threat Reduction Agency, upon receiving a request for notification of the existence of a record or for access to a record, shall acknowledge receipt of the request within 10 working days.

(b) Determine whether or not such record exists.

(c) Determine whether or not such request for access is available under the Privacy Act.

(d) Notify requester of determinations within 30 working days after receipt of such request.

(e) Provide access to information pertaining to that person which has been determined to be available within 30 working days.

(f) Notify the individual if fees will be assessed for reproducing copies of the records. Fee schedule and rules for assessing fees are contained in §318.11.

§ 318.8 Request for correction or amendment to a record.

(a) An individual may request that the Defense Threat Reduction Agency correct, amend, or expunge any record, or portions thereof, pertaining to the requester that he/she believe to be inaccurate, irrelevant, untimely, or incomplete.

(b) Such requests shall specify the particular portions of the records in question, be in writing and should be mailed to the FOIA/Privacy Act Division, Defense Threat Reduction Agency, 45045 Aviation Drive, Dulles, VA 20166–7517.

(c) The requester shall provide sufficient information to identify the record and furnish material to substantiate the reasons for requesting corrections, amendments, or expurgation.

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

(a) The Agency will acknowledge a request for correction or amendment within 10 working days of receipt. The acknowledgment will be in writing and will indicate the date by which the Agency expects to make its initial determination.

(b) The Agency shall complete its consideration of requests to correct or amend records within 30 working days, and inform the requester of its initial determination.

(c) If it is determined that records should be corrected or amended in whole or in part, the Agency shall advise the requester in writing of its determination; and correct or amend the records accordingly. The Agency shall then advise prior recipients of the records of the fact that a correction or amendment was made and provide the substance of the change.

(d) If the Agency determines that a record should not be corrected or amended, in whole or in part, as requested by the individual, the Agency shall advise the requester in writing of its refusal to correct or amend the records and the reasons therefor. The notification will inform the requester that the refusal may be appealed administratively and will advise the individual of the procedures for such appeals.

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

(a) An individual who disagrees with the denial or partial denial of his or

her request for access, correction, or amendment of Agency records pertaining the himself/herself, may file a request for administrative review of such refusal within 30 days after the date of notification of the denial or partial denial.

(b) Such requests shall be made in writing and mailed to the FOIA/Privacy Act Division, Defense Threat Reduction Agency, 45045 Aviation Drive, Dulles, VA 20166–7517.

(c) The requester shall provide a brief written statement setting for the reasons for his or her disagreement with the initial determination and provide such additional supporting material as the individual feels necessary to justify the appeal.

(d) Within 30 working days of receipt of the request for review, the Agency shall advise the individual of the final disposition of the request.

(e) In those cases where the initial determination is reversed, the individual will be so informed and the Agency will take appropriate action.

(f) In those cases where the initial determination is sustained, the individual shall be advised:

(1) In the case of a request for access to a record, of the individual's right to seek judicial review of the Agency refusal for access.

(2) In the case of a request to correct or amend the record:

(i) Of the individual's right to file a concise statement of his or her reasons for disagreeing with the Agency's decision in the record,

(ii) Of the procedures for filing a statement of the disagreement, and

(iii) Of the individual's right to seek judicial review of the Agency's refusal to correct or amend a record.

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

(a) General. No record contained in a system of records maintained by DTRA shall be disclosed by any means to any person or agency within or outside the Department of Defense without the request or consent of the subject of the record, except as described in 32 CFR 310.41, Appendix C to part 310, and/or a Defense Threat Reduction Agency system of records notice.

(b) Accounting of disclosures. Except for disclosures made to members of the DoD in connection with their official duties, and disclosures required by the Freedom of Information Act, an accounting will be kept of all disclosures of records maintained in DTRA system of records.

(1) Accounting entries will normally be kept on a DTRA form, which will be maintained in the record file jacket, or in a document that is part of the record.

(2) Accounting entries will record the date, nature and purpose of each disclosure, and the name and address of the person or agency to whom the disclosure is made.

(3) Accounting records will be maintained for at least 5 years after the last disclosure, of for the life of the record, whichever is longer.

(4) Subjects of DTRA records will be given access to associated accounting records upon request, except for those disclosures made to law enforcement activities when the law enforcement activity has requested that the disclosure not be made, and/or as exempted under § 318.16.

§ 318.12 Fees.

Individuals may request copies for retention of any documents to which they are granted access in DTRA records pertaining to them. Requesters will not be charged for the first copy of any records provided; however, duplicate copies will require a charge to cover costs of reproduction. Such charges will be computed in accordance with 32 CFR part 310.

§ 318.13 Enforcement actions.

Procedures and sanctions are set forth in 5 U.S.C. 552a, OMB Circular A–130, and 32 CFR part 310.

§ 318.14 Blanket routine uses.

(a) *Blanket routine uses.* Certain 'blanket routine uses' of the records have been established that are applicable to every record system maintained within the Department of Defense unless specifically stated otherwise within a particular record system. These additional blanket routine uses of the records are published only once in the interest of

simplicity, economy and to avoid redundancy.

(b) *Routine Use—Law Enforcement.* If a system of records maintained by a DoD Component, to carry out its functions, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether Federal, State, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

(c) *Routine Use—Disclosure When Requesting Information.* A record from a system of records maintained by a Component may be disclosed as a routine use to a Federal, State, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a Component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

(d) *Routine Use—Disclosure of Requested Information.* A record from a system of records maintained by a Component may be disclosed to a Federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

(e) *Routine Use—Congressional Inquiries.* Disclosure from a system of records maintained by a Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

(f) *Routine Use—Private Relief Legislation.* Relevant information contained in all systems of records of the Department of Defense published on or before August 22, 1975, will be disclosed to the OMB in connection with the review of private relief legislation as set forth in OMB Circular A–19 at any stage of the legislative coordination and clearance process as set forth in that Circular.

(g) *Routine Use—Disclosures Required by International Agreements.* A record from a system of records maintained by a Component may be disclosed to foreign law enforcement, security, investigatory, or administrative authorities to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements including those regulating the stationing and status in foreign countries of DoD military and civilian personnel.

(h) *Routine Use—Disclosure to State and Local Taxing Authorities.* Any information normally contained in Internal Revenue Service (IRS) Form W–2 which is maintained in a record from a system of records maintained by a Component may be disclosed to State and local taxing authorities with which the Secretary of the Treasury has entered into agreements under 5 U.S.C. 5516, 5517, and 5520 and only to those State and local taxing authorities for which an employee or military member is or was subject to tax regardless of whether tax is or was withheld. This routine use is in accordance with Treasury Fiscal Requirements Manual Bulletin No. 76–07.

(i) *Routine Use—Disclosure to the Office of Personnel Management.* A record from a system of records subject to the Privacy Act and maintained by a Component may be disclosed to the Office of Personnel Management (OPM) concerning information on pay and leave, benefits, retirement deduction, and any other information necessary for the OPM to carry out its legally authorized government-wide personnel management functions and studies.

(j) *Routine Use—Disclosure to the Department of Justice for Litigation.* A record from a system of records maintained by this component may be disclosed as a routine use to any component of the Department of Justice for

the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

(k) *Routine Use—Disclosure to Military Banking Facilities Overseas.* Information as to current military addresses and assignments may be provided to military banking facilities who provide banking services overseas and who are reimbursed by the Government for certain checking and loan losses. For personnel separated, discharged, or retired from the Armed Forces, information as to last known residential or home of record address may be provided to the military banking facility upon certification by a banking facility officer that the facility has a returned or dishonored check negotiated by the individual or the individual has defaulted on a loan and that if restitution is not made by the individual, the U.S. Government will be liable for the losses the facility may incur.

(l) *Routine Use—Disclosure of Information to the General Services Administration (GSA).* A record from a system of records maintained by this component may be disclosed as a routine use to the General Services Administration (GSA) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

(m) *Routine Use—Disclosure of Information to the National Archives and Records Administration (NARA).* A record from a system of records maintained by this component may be disclosed as a routine use to the National Archives and Records Administration (NARA) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

(n) Routine Use—Disclosure to the Merit Systems Protection Board. A record from a system of records maintained by this component may be disclosed as a routine use to the Merit Systems Protection Board, including the Office of the Special Counsel for the purpose of litigation, including administrative proceedings, appeals, special studies of the civil service and other merit systems, review of OPM or component rules and regulations, investigation of alleged or possible prohibited personnel practices; including administrative proceedings involving any individual subject of a DoD investigation, and such other functions, promulgated in 5 U.S.C. 1205 and 1206, or as may be authorized by law.

(o) *Routine Use—Counterintelligence Purpose.* A record from a system of records maintained by this component may be disclosed as a routine use outside the DoD or the U.S. Government for the purpose of counterintelligence activities authorized by U.S. Law or Executive Order or for the purpose of enforcing laws which protect the national security of the United States.

§ 318.15 Rules of conduct

(a) DTRA 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 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 32 CFR part 310 or other applicable law or regulation. Personnel willfully making such a disclosure when knowing the disclosure is prohibited are subject to possible criminal penalties and/or administrative sanctions.

(3) Report any unauthorized disclosure of personal information from a system of records or the maintenance of any system of records that are not authorized by the Instruction to the DTRA Privacy Act Officer.

(b) DTRA system managers for each system of records shall:

(1) Ensure that all personnel who either have access to the system of records or who shall develop or supervise procedures for the handling of records in the system of records shall be aware of their responsibilities for protecting personnel information being collected and maintained under the DTRA Privacy Program.

(2) Promptly notify the Privacy Act Officer of any required new, amended, or altered system notices for the system of records.

(3) Not maintain any official files on individuals, which are retrieved by

name or other personal identifier without first ensuring that a notice for the system of records shall have been published in the ''Federal Register.'' Any official who willfully maintains a system of records without meeting the publication requirements, as prescribed by 5 U.S.C. 552a, OMB Circular A–130, and 32 CFR part 310, is subject to possible criminal penalties and/or administrative sanctions.

§ 318.16 Exemption rules.

(a) *Exemption for classified material.* All systems of records maintained by the Defense Threat Reduction Agency shall be exempt under section (k)(1) of 5 U.S.C. 552a, to the extent that the systems contain any information properly classified under E.O. 12598 and that is required by that E.O. to be kept secret in the interest of national defense or foreign policy. This exemption is applicable to parts of all systems of records including those not otherwise specifically designated for exemptions herein which contain isolated items of properly classified information.

(b) *System identifier and name:* HDTRA 007, Security Operations.

(1) Exemption: Portions of this system of records may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d)(1) through (d)(4), (e)(1), (e)(4)(G), (H), (I), and (f).

(2) Authority: 5 U.S.C. 552a(k)(5).

(3) Reasons: (i) From subsection (c)(3) because it will enable DTRA to safeguard certain investigations and relay law enforcement information without compromise of the information, and protect the identities of confidential sources who might not otherwise come forward and who have furnished information under an express promise that the sources' identity would be held in confidence (or prior to the effective date of the Act, under an implied promise.)

(ii) From subsection (d)(1) through (d)(4) and (f) because providing access to records of a civil investigation and the right to contest the contents of those records and force changes to be made to the information contained therein would seriously interfere with and thwart the orderly and unbiased conduct of security investigations. Providing access rights normally afforded under the Privacy Act would provide the subject with valuable information that would allow interference with or compromise of witnesses or render witnesses reluctant to cooperate; lead to suppression, alteration, or destruction of evidence; and result in the secreting of or other disposition of assets that would make them difficult or impossible to reach in order to satisfy any Government claim growing out of the investigation or proceeding.

(iii) From subsection (e)(1), (e)(4)(G), (H), (I) because it will provide protection against notification of investigatory material including certain reciprocal investigations and counterintelligence information, which might alert a subject to the fact that an investigation of that individual is taking place, and the disclosure of which would weaken the on-going investigation, reveal investigatory techniques, and place confidential informants in jeopardy who furnished information; under an express promise that the sources' identity would be held in confidence (or prior to the effective date of the Act, under an implied promise.)

(c) *System identifier and name:* HDTRA 011, Inspector General Investigation Files.

(1) Exemption: Portions of this system of records may be exempt from the provisions of 5 U.S.C. 552a(c)(3); (d)(1) through (4); (e)(1); (e)(4)(G), (H), and (I); and (f).

(2) Authority: 5 U.S.C. 552a(k)(2).

(3) Reasons: (i) From subsection (c)(3) because it will enable DTRA to conduct certain investigations and relay law enforcement information without compromise of the information, protection of investigative techniques and efforts employed, and identities of confidential sources who might not otherwise come forward and who furnished information under an express promise that the sources' identity would be held in confidence (or prior to the effective date of the Act, under an implied promise.)

(ii) From subsection (d)(1) through (d)(4) and (f) because providing access to records of a civil investigation and the right to contest the contents of those records and force changes to be made to the information contained therein would seriously interfere with

and thwart the orderly and unbiased conduct of the investigation and impede case preparation. Providing access rights normally afforded under the Privacy Act would provide the subject with valuable information that would allow interference with or compromise of witnesses or render witnesses reluctant to cooperate; lead to suppression, alteration, or destruction of evidence; and result in the secreting of or other disposition of assets that would make them difficult or impossible to reach in order to satisfy any Government claim growing out of the investigation or proceeding.

(iii) From subsection (e)(1), (e)(4)(G), (H), and (I) because it will provide protection against notification of investigatory material including certain reciprocal investigations and counterintelligence information, which might alert a subject to the fact that an investigation of that individual is taking place, and the disclosure of which would weaken the on-going investigation, reveal investigatory techniques, and place confidential informants in jeopardy who furnished information under an express promise that the sources' identity would be held in confidence (or prior to the effective date of the Act, under an implied promise).

PART 319—DEFENSE INTELLIGENCE AGENCY PRIVACY PROGRAM

Sec.

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

SOURCE: 51 FR 44064, Dec. 8, 1986, unless otherwise noted. Redesignated at 56 FR 56595, Nov. 6, 1991 and 56 FR 57799, Nov. 14, 1991.

§319.1 Authority.

Pursuant to the requirements of section 553 of Title 5 of the United States Code, the Defense Intelligence Agency promulgates its rules for the implementation of the Privacy Act of 1974, Pub. L. 93–579, 5 U.S.C. 552a (f) and (k).

§319.2 Purpose.

(a) To promulgate rules providing procedures by which individuals may exercise their rights granted by the act to:

(1) Determine whether a Defense Intelligence Agency system of records contains a record pertaining to themselves;

(2) Be granted access to all or portions thereof;

(3) Request administrative correction or amendment of such records;

(4) Request an accounting of disclosures from such records; and

(5) Appeal any adverse determination for access or correction/amendment of records.

(b) To set forth Agency policy and fee schedule for cost of duplication.

(c) To identify records subject to the provisions of these rules.

(d) To specify those systems of records for which the Director, Defense Intelligence Agency, claims an exemption.

§319.3 Scope.

(a) Any individual who is a citizen of the United States or an alien lawfully admitted for permanent residence in the United States may submit an inquiry to the Defense Intelligence Agency.

(b) These rules apply to those systems of records:

(1) Maintained by the Defense Intelligence Agency;

(2) For which the Defense Intelligence Agency prescribes the content and disposition pursuant to statute or executive order of the President, which may be in the physical custody of another Federal agency;

(3) Not exempted from certain provisions of the act by the Director, Defense Intelligence Agency.