SUBCHAPTER O—PRIVACY PROGRAM

PART 310—DOD PRIVACY PROGRAM

Subpart A—DoD Policy

Subpart B—Systems of Records

Subpart C—Collecting Personal Information

Subpart D—Access by Individuals

Subpart E—Disclosure of Personal Information to Other Agencies and Third Parties

Subpart F—Exemptions

Subpart G—Publication Requirements

Subpart H—Training Requirements

Subpart I—Reports

Subpart J—Inspections

Subpart K—Privacy Act Violations

Subpart L—Computer Matching Program Procedures

AUTHORITY: 5 U.S.C. 552a.

SOURCE: 72 FR 18758, Apr. 13, 2007, unless otherwise noted.

Subpart A—DoD Policy

§ 310.1 Reissuance.

This part consolidates into a single location (32 CFR part 310) Department of Defense (DoD) policies and procedures for implementing the Privacy Act of 1974, as amended (5 U.S.C. 552a) by authorizing the development, publication and maintenance of the DoD Privacy Program set forth by DoD Directive 5400.11[1] and 5400.11–R,[2] both entitled: ''DoD Privacy Program.''

§ 310.2 Purpose.

This part:

(a) Updates the established policies and assigned responsibilities of the DoD Privacy Program pursuant to 5 U.S.C. 552a (also known and referred to in this part as ''The Privacy Act'') and Office of Management and Budget (OMB) Circular No. A–130.

(b) Authorizes the Defense Privacy Board and the Defense Data Integrity Board.

(c) Prescribes uniform procedures for implementation of and compliance with the DoD Privacy Program.

(d) Delegates authorities and responsibilities for the effective administration of the DoD Privacy Program.

[80 FR 4207, Jan. 27, 2015]

§ 310.3 Applicability and scope.

(a) This part applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this part as the ''DoD Components'').

(b) For the purposes of subsection (i), ''Criminal penalties,'' of The Privacy Act, any DoD contractor and any employee of such a contractor will be considered to be an employee of DoD when DoD provides by a contract for the operation by or on behalf of DoD of a system of records to accomplish a DoD function. DoD will, consistent with its authority, cause the requirements of section (m) of The Privacy Act to be applied to such systems.

[80 FR 4207, Jan. 27, 2015]

§ 310.4 Definitions.

The following definitions apply to this part:

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 the DoD Components, the Department of Defense is considered a single agency. For all other purposes to include requests for access and amendment, denial of access or amendment, appeals from denials, and record keeping as relating to release of records to non-DoD Agencies, each DoD Component is considered an agency within the meaning of the Privacy Act.

Breach. A loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information (PII), whether physical or electronic.

Computer matching. The computerized comparison of two or more automated systems of records or a system of records with non-federal records. Manual comparisons are not covered.

Confidential source. A person or organization who has furnished information to the Federal Government under an express promise, if made on or after September 27, 1975, that the person's or the organization's identity shall be held in confidence or under an implied promise of such confidentiality if this implied promise was made on or before September 26, 1975.

Disclosure. The information sharing or transfer of any PII from a system of records by any means of communication (such as oral, written, electronic, mechanical, or actual review) to any person, government agency, or private entity other than the subject of the

[1] Copies may be obtained at *http://www.dtic.mil/whs/directives.*

[2] See footnote 1 to § 310.1.

record, the subject's designated agent, or the subject's legal guardian.

DoD contractor. Any individual or other legal entity that:

(1) Directly or indirectly (*e.g.*, through an affiliate) submits offers for or is awarded, or reasonably may be expected to submit offers for or be awarded, a government contract, including a contract for carriage under government or commercial bills of lading, or a subcontract under a government contract; or

(2) Conducts business, or reasonably may be expected to conduct business, with the federal government as an agent or representative of another contractor.

DoD personnel. Service members and federal civilian employees.

Federal benefit program. A program administered or funded by the Federal Government, or by any agent or State on behalf of the Federal Government, providing cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to individuals.

Federal personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits).

Individual. A living person who is a U.S. citizen 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, except as otherwise provided in this part. Members of the Military Services are ''individuals.'' Corporations, partnerships, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities are not ''individuals'' when acting in an entrepreneurial capacity with the DoD, but persons employed by such organizations or entities are ''individuals'' when acting in a personal capacity (*e.g.*, security clearances, entitlement to DoD privileges or benefits).

Individual access. Access to information pertaining to the individual by the individual or his or her designated agent or legal guardian.

Information sharing environment. Defined in Public Law 108–458, ''The Intelligence Reform and Terrorism Prevention Act of 2004''.

Lost, stolen, or compromised information. Actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purpose where one or more individuals will be adversely affected. Such incidents also are known as breaches.

Maintain. The collection, maintenance, use, or dissemination of records contained 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.

Mixed system of records. Any system of records that contains information about individuals as defined by the Privacy Act and non-U.S. citizens and/or aliens not lawfully admitted for permanent residence.

Non-Federal agency. Any state or local government, or agency thereof, which receives records contained in a system of records from a source agency for use in a computer matching program.

Official use. Within the context of this part, this term is used when officials and employees of a DoD Component have a demonstrated a need for the record or the information contained therein in the performance of their official duties, subject to DoD 5200.1–R.[3]

Personally identifiable information (PII). Information used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, biometric records, home phone numbers, other demographic, personnel, medical, and financial information. PII includes any information that is linked or linkable to a specified individual, alone, or when combined with other personal or identifying information. For purposes of this part, the

[3] See footnote 1 to § 310.1

term PII also includes personal information and information in identifiable form.

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.

Protected health information (PHI). Defined in DoD 6025.18–R, ''DoD Health Information Privacy Regulation'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/602518r.pdf*).

Recipient agency. Any agency, or contractor thereof, receiving records contained in a system of records from a source agency for use in a computer matching program.

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

Risk assessment. An analysis considering information sensitivity, vulnerabilities, and cost 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.

Source agency. Any agency which discloses records contained in a system of records to be used in a computer matching program, or any state or local government, or agency thereof, which discloses records to be used in a computer matching program.

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

System of records notice (SORN). A notice published in the FEDERAL REGISTER that constitutes official notification to the public of the existence of a system of records.

[80 FR 4207, Jan. 27, 2015]

§ 310.5 Policy.

It is DoD policy that:

(a) An individual's privacy is a fundamental legal right that must be respected and protected.

(1) The DoD's need to collect, use, maintain, or disseminate (also known and referred to in this part as ''maintain'') PII about individuals for purposes of discharging its statutory responsibilities will be balanced against their right to be protected against unwarranted privacy invasions.

(2) The DoD protects individuals' rights, consistent with federal laws, regulations, and policies, when maintaining their PII.

(3) DoD personnel and DoD contractors have an affirmative responsibility to protect an individual's privacy when maintaining his or her PII.

(4) Consistent with section 1016(d) of Public Law 108–458 and section 1 of Executive Order 13388, ''Further Strengthening the Sharing of Terrorism Information to Protect Americans'', the DoD will protect information privacy and provide other protections relating to civil liberties and legal rights in the development and use of the information sharing environment.

(b) The DoD establishes rules of conduct for DoD personnel and DoD contractors involved in the design, development, operation, or maintenance of any system of records. DoD personnel and DoD contractors will be trained with respect to such rules and the requirements of this section and any other rules and procedures adopted pursuant to this section and the penalties for noncompliance. The DoD Rules of Conduct are established in § 310.8.

(c) DoD personnel and DoD contractors conduct themselves consistent with the established rules of conduct in § 310.8, so that records maintained in a system of records will only be maintained as authorized by 5 U.S.C. 552a and this part.

(d) DoD legislative, regulatory, or other policy proposals will be evaluated to ensure consistency with the information privacy requirements of this part.

(e) Pursuant to The Privacy Act, no record will be maintained on how an individual exercises rights guaranteed by the First Amendment to the Constitution of the United States (referred to in this part as ''the First Amendment''), except:

(1) When specifically authorized by statute.

(2) When expressly authorized by the individual that the record is about.

(3) When the record is pertinent to and within the scope of an authorized law enforcement activity, including an authorized intelligence or administrative investigation.

(f) Disclosure of records pertaining to an individual from a system of records is prohibited except with his or her consent or as otherwise authorized by 5 U.S.C. 552a and this part or 32 CFR part 286. When DoD Components make such disclosures, the individual may, to the extent authorized by 5 U.S.C. 552a and this part, obtain a description of such disclosures from the Component concerned.

(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 is prohibited to the extent authorized by Public Law 86–36, ''National Security Agency-Officers and Employees'' and 10 U.S.C. 424. Disclosure of records pertaining to personnel of overseas, sensitive, or routinely deployable units is prohibited to the extent authorized by 10 U.S.C. 130b.

(h) The DoD establishes appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is maintained.

(i) Disclosure of PHI will be consistent with DoD 6025.18–R.

(j) All DoD personnel and DoD contractors will be provided training pursuant to 5 U.S.C. 552a and OMB Circular No. A–130.

(k) PII collected, used, maintained, or disseminated will be:

(1) Relevant and necessary to accomplish a lawful DoD purpose required by statute or Executive Order.

(2) Collected to the greatest extent practicable directly from the individual. He or she will be informed as to why the information is being collected, the authority for collection, how it will be used, whether disclosure is mandatory or voluntary, and the consequences of not providing that information.

(3) Relevant, timely, complete, and accurate for its intended use.

(4) Protected using appropriate administrative, technical, and physical safeguards based on the media (*e.g.*, paper, electronic) involved. Protection will ensure the security of the records and prevent compromise or misuse during maintenance, including working at authorized alternative worksites.

(l) Individuals are permitted, to the extent authorized by 5 U.S.C. 552a and this part, to:

(1) Upon request by an individual, gain access to records or to any information pertaining to the individual which is contained in a system of records.

(2) Obtain a copy of such records, in whole or in part.

(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 for a request to access or a request to amend a record.

(m) Non-U.S. citizens and aliens not lawfully admitted for permanent residence may request access to and amendment of records pertaining to them; however, this part does not create or extend any right pursuant to The Privacy Act to them.

(n) SORNs and notices of proposed or final rulemaking are published in the FEDERAL REGISTER (FR), and reports

are submitted to Congress and OMB, in accordance with 5 U.S.C. 552a, OMB Circular No. A–130, and this part, Volume 1 of DoD Manual 8910.01, ''DoD Information Collections Manual: Procedures for DoD Internal Information Collections'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/891001m_vol1.pdf*), and DoD Instruction 5545.02, ''DoD Policy for Congressional Authorization and Appropriations Reporting Requirements'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/554502p.pdf*). Information about an individual maintained in a new system of records will not be collected until the required SORN publication and review requirements are satisfied.

(o) All DoD personnel must make reasonable efforts to inform an individual, at their last known address, when any record about him or her is disclosed:

(1) Due to a compulsory legal process.

(2) In a manner that will become a matter of public record.

(p) Individuals must be notified in a timely manner, consistent with the requirements of this part, if there is a breach of their PII.

(q) At least 30 days prior to disclosure of information pursuant to subparagraph (e)(4)(D) (routine uses) of The Privacy Act, the DoD will publish an FR notice of any new use or intended use of the information in the system, and provide an opportunity for interested people to submit written data, views, or arguments to the agency.

(r) Computer matching programs between the DoD Components and federal, state, or local governmental agencies are conducted in accordance with the requirements of 5 U.S.C. 552a, OMB Circular No. A–130, and this part.

(s) The DoD will publish in the FR notice any establishment or revision of a matching program at least 30 days prior to conducting such program of such establishment or revision if any DoD Component is a recipient agency or a source agency in a matching program with a non-federal agency.

[80 FR 4208, Jan. 27, 2015]

§ 310.6 Responsibilities.

(a) The Deputy Chief Management Officer of the Department of Defense (DCMO):

(1) Serves as the Senior Agency Official for Privacy (SAOP) for the DoD. These duties, in accordance with OMB Memorandum M–05–08, ''Designation of Senior Agency Officials for Privacy'' (available at *http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-08.pdf*), include:

(i) Ensuring DoD implementation of information privacy protections, including full compliance with federal laws, regulations, and policies relating to information privacy.

(ii) Overseeing, coordinating, and facilitating DoD privacy compliance efforts.

(iii) Ensuring that DoD personnel and DoD contractors receive appropriate training and education programs regarding the information privacy laws, regulations, policies, and procedures governing DoD-specific procedures for handling of PII.

(2) Provides rules of conduct and policy for, and coordinates and oversees administration of, the DoD Privacy Program to ensure compliance with policies and procedures in 5 U.S.C. 552a and OMB Circular No. A–130.

(3) Publishes this part and other guidance to ensure timely and uniform implementation of the DoD Privacy Program.

(4) Serves as the chair of the Defense Privacy Board and the Defense Data Integrity Board.

(5) As requested, ensures that guidance, assistance, and subject matter expert support are provided to the Combatant Command privacy officers in the implementation and execution of and compliance with the DoD Privacy Program.

(6) Acts as The Privacy Act Access and Amendment appellate authority for OSD and the Office of the Chairman of the Joint Chiefs of Staff when an individual is denied access to or amendment of records pursuant to The Privacy Act, DoD Directive 5105.53, ''Director of Administration and Management (DA&M)'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/510553p.pdf*), and Deputy Secretary of

Defense Memorandum, ''Reorganization of the Office of the Deputy Chief Management Officer.''

(b) Under the authority, direction, and control of the DCMO, through the Director for Oversight and Compliance, the Chief, Defense Privacy and Civil Liberties Division (DPCLD):

(1) Ensures that laws, policies, procedures, and systems for protecting individual privacy rights are implemented throughout DoD.

(2) Oversees and provides strategic direction for the DoD Privacy Program.

(3) Assists the DCMO in performing the responsibilities in paragraphs (a)(1)–(a)(6) of this section.

(4) Reviews DoD legislative, regulatory, and other policy proposals that contain information on privacy issues relating to how the DoD keeps its PII. These reviews must include any proposed legislation, testimony, and comments having privacy implications in accordance with DoD Directive 5500.01, ''Preparing, Processing, and Coordinating Legislation, Executive Orders, Proclamations, Views Letters, and Testimony'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/550001p.pdf*).

(5) Reviews proposed new, altered, and amended systems of records. Submits required SORNs for publication in the FR and, when required, provides advance notification to OMB and Congress consistent with 5 U.S.C. 552a, OMB Circular No. A–130, and this part.

(6) Reviews proposed DoD Component privacy exemption rules. Submits the exemption rules for publication in the FR, and submits reports to OMB and Congress consistent with 5 U.S.C. 552a, OMB Circular No. A–130, and this part.

(7) Develops, coordinates, and maintains all DoD computer matching agreements. Submits required match notices for publication in the FR and provides advance notification to OMB and Congress consistent with 5 U.S.C. 552a, OMB Circular No. A–130, and this part.

(8) Provides guidance, assistance, and support to the DoD Components in their implementation of the DoD Privacy Program to ensure that:

(i) All requirements developed to maintain PII conform to the DoD Privacy Program standards.

(ii) Appropriate procedures and safeguards are developed and implemented to protect PII when it is collected, used, maintained, or disseminated in any media.

(iii) Specific procedures and safeguards are developed and implemented when PII is collected and maintained for research purposes.

(9) Compiles data in support of the DoD Chief Information Officer (DoD CIO) submission of the Federal Information Security Management Act (FISMA) Privacy Reports, pursuant to OMB Memorandum M–06–15, ''Safeguarding Personally Identifiable Information'' (available at *http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m-06-15.pdf*); the Biennial Matching Activity Report to OMB, in accordance with OMB Circular No. A–130 and this part; the semiannual Section 803 report in accordance with 42 U.S.C. 2000ee and 2000ee–1; and other reports as required.

(10) Reviews and coordinates on DoD Component privacy program implementation rules to ensure they are in compliance with the DoD-level guidance.

(11) Provides operational and administrative support to the Defense Privacy Board and the Defense Data Integrity Board.

(c) The General Counsel of the Department of Defense (GC DoD):

(1) Provides advice and assistance on all legal matters related to the administration of the DoD Privacy Program.

(2) Appoints a designee to serve as a member of the Defense Privacy Board and the Defense Data Integrity Board.

(3) When a DoD Privacy Program group is created, appoints a designee to serve as a member.

(d) The DoD Component heads:

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

(2) Establish DoD Component-specific procedures in compliance with this part and publish these procedures as well as rules of conduct in the FR.

(3) Establish and implement appropriate administrative, physical, and technical safeguards and procedures prescribed in this part and other DoD Privacy Program guidance.

(4) Ensure Component compliance with supplemental guidance and procedures in accordance with all applicable federal laws, regulations, policies, and procedures.

(5) Appoint a Component senior official for privacy (CSOP) to support the SAOP in carrying out the SAOP's duties identified in OMB Memorandum M–05–08.

(6) Appoint a Component privacy officer to administer the DoD Privacy Program, on behalf of the CSOP.

(7) Ensure DoD personnel and DoD contractors having primary responsibility for implementing the DoD Privacy Program receive appropriate privacy training. This training must be consistent with the requirements of this part and will address the provisions of 5 U.S.C. 552a, OMB Circular No. A–130, and this part.

(8) Ensure that all DoD Component legislative, regulatory, or other policy proposals are evaluated to ensure consistency with the information privacy requirements of this part.

(9) Assess the impact of technology on the privacy of PII and, when feasible, adopt privacy-enhancing technology to:

(i) Preserve and protect PII contained in a DoD Component system of records.

(ii) Audit compliance with the requirements of this part.

(10) Ensure that officials who have specialized knowledge of the DoD Privacy Program periodically review Component implementation of and compliance with the DoD Privacy Program.

(11) Submit reports, consistent with the requirements of this part, in accordance with 5 U.S.C. 552a and OMB Circular No. A–130, and as otherwise directed by the Chief, DPCLD.

(e) In addition to the responsibilities in paragraph (d), the Secretaries of the Military Departments provide program and financial support to the Combatant Commands as identified in DoD Directive 5100.03, ''Support to the Headquarters of Combatant and Subordinate Unified Commands'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/510003p.pdf*) to fund, without reimbursement, the administrative and logistic support required by combatant and subordinate unified command headquarters to perform their assigned missions effectively.

[80 FR 4209, Jan. 27, 2015]

§ 310.7 [Reserved]

§ 310.8 Rules of conduct.

In accordance with section (e)(9) of The Privacy Act, this section provides DoD rules of conduct for the development, operation, and maintenance of systems of records. DoD personnel and DoD contractor personnel will:

(a) Take action to ensure that any PII contained in a system of records that they access and use to conduct official business will be protected so that the security and confidentiality of the information is preserved.

(b) Not disclose any PII contained in any system of records, except as authorized by The Privacy Act, or other applicable statute, Executive order, regulation, or policy. Those willfully making any unlawful or unauthorized disclosure, knowing that disclosure is prohibited, may be subject to criminal penalties and/or administrative sanctions.

(c) Report any unauthorized disclosures of PII from a system of records to the applicable Privacy point of contact (POC) for the respective DoD Component.

(d) Report the maintenance of any system of records not authorized by this part to the applicable Privacy POC for the respective DoD Component.

(e) Minimize the collection of PII to that which is relevant and necessary to accomplish a purpose of the DoD.

(f) Not maintain records describing how any individual exercises rights guaranteed by the First Amendment, except:

(1) When specifically authorized by statute.

(2) When expressly authorized by the individual that the record is about.

(3) When the record is pertinent to and within the scope of an authorized law enforcement activity, including authorized intelligence or administrative activities.

(g) Safeguard the privacy of all individuals and the confidentiality of all PII.

(h) Limit the availability of records containing PII to DoD personnel and

DoD contractors who have a need to know in order to perform their duties.

(i) Prohibit unlawful possession, collection, or disclosure of PII, whether or not it is within a system of records.

(j) Ensure that all DoD personnel and DoD contractors who either have access to a system of records or develop or supervise procedures for handling records in a system of records are aware of their responsibilities and are properly trained to safeguard PII being maintained under the DoD Privacy Program.

(k) Prepare any required new, amended, or altered SORN for a given system of records and submit the SORN through their DoD Component Privacy POC to the Chief, DPCLD, for coordination and submission for publication in the FR.

(l) Not maintain any official files on individuals, which are retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual, also known as a system of records, without first ensuring that a notice has been published in the FR. Any official who willfully maintains a system of records without meeting the publication requirements as prescribed by this part and The Privacy Act may be subject to criminal penalties and/or administrative sanctions.

(m) Maintain all records in a mixed system of records as if all the records in such a system are subject to The Privacy Act.

[80 FR 4210, Jan. 27, 2015]

§310.9 Privacy boards and office, composition and responsibilities.

(a) *The Defense Privacy Board*—(1) *Membership*. The Board consists of:

(i) *Voting members*. Representatives designated by the Secretaries of the Military Departments and the following officials or their designees:

(A) The DCMO, who serves as the chair.

(B) The Chief, DPCLD, who serves as the Executive Secretary and as a member.

(C) The Under Secretary of Defense for Personnel and Readiness.

(D) The Assistant Secretary of Defense for Health Affairs.

(E) The DoD CIO.

(F) The Director, Defense Manpower Data Center.

(G) The Director, Executive Services Directorate, Washington Headquarters Services (WHS).

(H) The GC DoD.

(I) The Chief of the National Guard Bureau.

(ii) *Non-voting members*. Non-voting members are the Director, Enterprise Information Technology Services Directorate (EITSD), WHS; and the representatives designated by Defense Agency and DoD Field Activity directors.

(2) *Responsibilities*. The Board:

(i) Serves as the primary DoD policy forum for matters involving the DoD Privacy Program, meeting as necessary to address issues of common concern to ensure that consistent policy is adopted and followed by the DoD Components. The Board issues advisory opinions, as necessary, on the DoD Privacy Program to promote uniform and consistent application of 5 U.S.C. 552a, OMB Circular No. A–130, and this part.

(ii) Establishes and convenes committees as necessary.

(iii) Establishes working groups whose membership is composed of DoD Component privacy officers and others as necessary.

(b) *The Defense Data Integrity Board*—(1) *Membership*. The Board consists of:

(i) The DCMO, who serves as the chair.

(ii) The Chief, DPCLD, who serves as the Executive Secretary.

(iii) The representatives designated by the Secretaries of the Military Departments; the DoD CIO; the GC DoD; the Inspector General of the Department of Defense, who is a non-voting advisory member; the Director, EITSD; and the Director, Defense Manpower Data Center.

(2) *Responsibilities*. The Board:

(i) Oversees and coordinates, consistent with the requirements of 5 U.S.C. 552a, OMB Circular No. A–130, and this part, all computer matching agreements involving personal records contained in systems of records maintained by the DoD Components.

(ii) Reviews and approves all computer matching agreements between the DoD and other federal, state, or local governmental agencies, as well as

any memorandums of understanding, when the match is internal to the DoD. This review ensures that, in accordance with 5 U.S.C. 552a, OMB Circular No. A–130, and this part, appropriate procedural and due process requirements are established before engaging in computer matching activities.

(c) *The Defense Privacy Board Legal Committee*—(1) *Membership.* The Committee shall consist of the Director, DPO, DA&M, who shall serve as the Chair and the Executive Secretary; the GC, DoD, or designee; and civilian and/or military counsel from each of the DoD Components. The General Counsels (GCs) and The Judge Advocates General of the Military Departments shall determine who shall provide representation for their respective Department to the Committee. This does not preclude representation from each office. The GCs of the other DoD Components shall provide legal representation to the Committee. Other DoD civilian or military counsel may be appointed by the Executive Secretary, after coordination with the DoD Component concerned, to serve on the Committee on those occasions when specialized knowledge or expertise shall be required.

(2) *Responsibilities.* (i) The Committee shall serve as the primary legal forum for addressing and resolving all legal issues arising out of or incident to the operation of the DoD Privacy Program.

(ii) The Committee shall consider legal questions regarding the applicability of 5 U.S.C. 552a, OMB Circular A–130, and DoD 5400.11–R and questions arising out of or as a result of other statutory and regulatory authority, to include the impact of judicial decisions, on the DoD Privacy Program. The Committee shall provide advisory opinions to the Defense Privacy Board and, on request, to the DoD Components.

(d) *The DPO*—(1) *Membership.* It shall consist of a Director and a staff. The Director also shall serve as the Executive Secretary and a member of the Defense Privacy Board; as the Executive Secretary to the Defense Data Integrity Board; and as the Chair and the Executive Secretary to the Defense Privacy Board Legal Committee.

(2) *Responsibilities.* (i) Manage activities in support of the Privacy Program oversight responsibilities of the DA&M.

(ii) Provide operational and administrative support to the Defense Privacy Board, the Defense Data Integrity Board, and the Defense Privacy Board Legal Committee.

(iii) Direct the day-to-day activities of the DoD Privacy Program.

(iv) Provide guidance and assistance to the DoD Components in their implementation and execution of the DoD Privacy Program.

(v) Review DoD legislative, regulatory, and other policy proposals which implicate information privacy issues relating to the Department's collection, maintenance, use, or dissemination of personal information, to include any testimony and comments having such implications under DoD Directive 5500.1.

(vi) Review proposed new, altered, and amended systems of records, to include submission of required notices for publication in the FEDERAL REGISTER and, when required, providing advance notification to the OMB and the Congress, consistent with 5 U.S.C. 552a, OMB Circular A–130, and DoD 5400.11–R.

(vii) Review proposed DoD Component privacy rulemaking, to include submission of the rule to the Office of the Federal Register for publication and providing to the OMB and the Congress reports, consistent with 5 U.S.C. 552a, OMB Circular A–130, and DoD 5400.11–R.

(viii) Develop, coordinate, and maintain all DoD computer matching agreements, to include the submission of required match notices for publication in the FEDERAL REGISTER and the provision of advance notification to the OMB and the Congress, consistent with 5 U.S.C. 552a, OMB Circular A–130, and DoD 5400.11–R.

(ix) Provide advice and support to the DoD Components to ensure:

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

(B) 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

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

(x) Serve as the principal POC for coordination of privacy and related matters with the OMB and other Federal, State, and local governmental agencies.

(xi) Compile and submit the ''Biennial Matching Activity Report'' to the OMB as required by OMB Circular A–130 and DoD 5400.11–R, and the Quarterly and Annual Federal Information Security Management Agency (FISMA) Privacy Reports, as required by 44 U.S.C. 3544(c), such other reports as may be required.

(xii) Update and maintain this part and DoD 5400.11–R.

[72 FR 18758, Apr. 13, 2007, as amended at 80 FR 4211, Jan. 27, 2015]

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 310.4(r)) 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 retrieved by name or other personal identifier to become a system of records for the purpose of this part.

(i) When records are contained in an automated (Information Technology) system that is capable of being manipulated to retrieve information about an individual, this does not automatically transform the system into a system of records as defined in this part.

(ii) In determining whether an automated system is a system of records that is subject to this part, retrieval policies and practices shall be evaluated. If DoD Component policy is to retrieve personal information by the name or other unique personal identifier, it is a system of records. If DoD Component policy prohibits retrieval by name or other identifier, but the actual practice of the Component is to retrieve information by name or identifier, even if done infrequently, it is a system of records.

(2) If records are retrieved by name or personal identifier, a system notice must be submitted in accordance with § 310.33.

(3) If records are not retrieved by name or personal identifier but then are rearranged in such a manner that they are retrieved by name or personal identifier, a new systems notice must be submitted in accordance with § 310.33.

(4) 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 § 310.34.

(c) *Relevance and necessity.* Information or records about an individual shall only be maintained in a system of records that is relevant and necessary to accomplish a DoD Component 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 authorizes 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. If a statute or Executive Order does not expressly direct the creation of a system of records, but the establishment of a system of records is necessary in order to discharge the requirements of the statute or Executive Order, the statute or Executive Order shall be cited as authority.

(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 alteration or amendment is prepared (see § 310.33 and § 310.34).

(2) Consider the following:

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

(ii) The specific impact on the purpose or mission of not collecting each category of information contained in the system;

(iii) The possibility of meeting the informational requirements through use of information not individually identifiable or through other techniques, such as sampling;

(iv) The length of time each item of personal information must be retained;

(v) The cost of maintaining the information; and

(vi) The necessity and relevancy of the information to the purpose for which it was collected.

(g) *Discontinued information requirements.* (1) Stop collecting immediately any category or item of personal information for which retention is no longer justified. Also delete this information from existing records, when feasible.

(2) Do not destroy any records that must be retained in accordance with disposal authorizations established under 44 U.S.C. 3303a, Examination by Archivist of Lists and Schedules of Records Lacking Preservation Value; Disposal of Records.''

§ 310.11 Standards of accuracy.

(a) *Accuracy of information maintained.* Maintain all personal information used or may be used to make any determination about an individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual in making any such determination.

(b) *Accuracy determinations before dissemination.* Before disseminating any personal information from a system of records to any person outside the Department of Defense, other than a Federal Agency, make reasonable efforts to ensure the information to be disclosed is accurate, relevant, timely, and complete for the purpose it is being maintained (see § 310.21(d)).

§ 310.12 Government contractors.

(a) *Applicability to government contractors.* (1) When a DoD Component contract requires the operation or maintenance of a system of records or a portion of a system of records or requires the performance of any activities associated with maintaining a system of records, including the collection, use, and dissemination of records, the record system or the portion of the record system affected are considered to be maintained by the DoD Component and are subject to this part. The Component is responsible for applying the requirements of this part to the contractor. The contractor and its employees are to be considered employees of the DoD Component for purposes of the criminal provisions of 5 U.S.C 552a(i) during the performance of the contract. Consistent with the Federal Acquisition Regulation (FAR), Part 24.1, contracts requiring the maintenance or operation of a system of records or the portion of a system of records shall include in the solicitation and resulting contract such terms as are prescribed by the FAR.

(2) If the contractor must use, have access to, or disseminate individually identifiable information subject to this part in order to perform any part of a contract, and the information would have been collected, maintained, used, or disseminated by the DoD Component but for the award of the contract, these

contractor activities are subject to this part.

(3) The restriction in paragraphs (a)(1) and (2) of this section do not apply to records:

(i) Established and maintained to assist in making internal contractor management decisions, such as records maintained by the contractor for use in managing the contract;

(ii) Maintained as internal contractor employee records even when used in conjunction with providing goods and services to the Department of Defense; or

(iii) Maintained as training records by an educational organization contracted by a DoD Component to provide training when the records of the contract students are similar to and commingled with training records of other students (for example, admission forms, transcripts, academic counseling and similar records).

(iv) Maintained by a consumer reporting agency to which records have been disclosed under contract in accordance with the Federal Claims Collection Act of 1966, 31 U.S.C. 3711(e).

(v) Maintained by the contractor incident to normal business practices and operations.

(4) The DoD Components shall publish instructions that:

(i) Furnish DoD Privacy Program guidance to their personnel who solicit, award, or administer Government contracts;

(ii) Inform prospective contractors of their responsibilities, and provide training as appropriate, regarding the DoD Privacy Program; and

(iii) Establish an internal system of contractor performance review to ensure compliance with the DoD Privacy Program.

(b) *Contracting procedures.* The Defense Acquisition Regulations Council shall develop the specific policies and procedures to be followed when soliciting bids, awarding contracts or administering contracts that are subject to this part.

(c) *Contractor compliance.* Through the various contract surveillance programs, ensure contractors comply with the procedures established in accordance with § 310.12(b).

(d) *Disclosure of records to contractors.* Disclosure of records contained in a system of records by a DoD Component to a contractor for use in the performance of a DoD contract is considered a disclosure within the Department of Defense (see § 310.21(b)). The contractor is considered the agent of the contracting DoD Component and to be maintaining and receiving the records for that Component.

§ 310.13 Safeguarding personal information.

(a) *General responsibilities.* DoD Components shall establish appropriate administrative, technical and physical safeguards to ensure that the records in each system of records are protected from unauthorized access, alteration, or disclosure and that their confidentiality is preserved and protected. Records shall be protected against reasonably anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is kept.

(b) *Minimum standards.* (1) Tailor system safeguards to conform to the type of records in the system, the sensitivity of the personal information stored, the storage medium used and, to a degree, the number of records maintained.

(2) Treat all unclassified records that contain personal information that normally would be withheld from the public under Freedom of Information Exemption Numbers 6 and 7 of 286.12, subpart C of 32 CFR part 286 (''DoD Freedom of Information Act Program'') as ''For Official Use Only,'' and safeguard them accordingly, in accordance with DoD 5200.1–R even if they are not actually marked ''For Official Use Only.''

(3) Personal information that does not meet the criteria discussed in paragraph (b)(2) of this section shall be accorded protection commensurate with the nature and type of information involved.

(4) Special administrative, physical, and technical procedures are required to protect data that is stored or processed in an information technology system to protect against threats unique to an automated environment (see appendix A).

(5) Tailor safeguards specifically to the vulnerabilities of the system.

(c) *Records disposal.* (1) Dispose of records containing personal data so as to prevent inadvertent compromise. Disposal methods are those approved by the Component or the National Institute of Standards and Technology. For paper records, disposal methods, such as tearing, burning, melting, chemical decomposition, pulping, pulverizing, shredding, or mutilation are acceptable. For electronic records, and media, disposal methods, such as overwriting, degaussing, disintegration, pulverization, burning, melting, incineration, shredding or sanding, are acceptable.

(2) Disposal methods are considered adequate if the personal data is rendered unrecognizable or beyond reconstruction.

§ 310.14 Notification when information is lost, stolen, or compromised.

(a) If records containing personal information are lost, stolen, or compromised, the potential exists that the records may be used for unlawful purposes, such as identity theft, fraud, stalking, etc. The personal impact on the affected individual may be severe if the records are misused. To assist the individual, the Component shall promptly notify the individual of any loss, theft, or compromise (See also, § 310.50 for reporting of the breach to Senior Component Official for Privacy and the Defense Privacy Office).

(1) The notification shall be made whenever a breach occurs that involves personal information pertaining to a service member, civilian employee (appropriated or non-appropriated fund), military retiree, family member, DoD contractor, other persons that are affiliated with the Component (e.g., volunteer), and/or any other member of the public on whom information is maintained by the Component or by a contractor on behalf of the Component.

(2) The notification shall be made as soon as possible, but not later than 10 working days after the loss, theft, or compromise is discovered and the identities of the individuals ascertained.

(i) The 10 day period begins to run after the Component is able to determine the identities of the individuals whose records were lost.

(ii) If the Component is only able to identify some but not all of the affected individuals, notification shall be given to those that can be identified with follow-up notifications made to those subsequently identified.

(iii) If the Component cannot readily identify the affected individuals or will not be able to identify the individuals, the Component shall provide a generalized notice to the potentially impacted population by whatever means the Component believes is most likely to reach the affected individuals.

(3) When personal information is maintained by a DoD contractor on behalf of the Component, the contractor shall notify the Component immediately upon discovery that a loss, theft or compromise has occurred.

(i) The Component shall determine whether the Component or the contractor shall make the required notification.

(ii) If the contractor is to notify the impacted population, it shall submit the notification letters to the Component for review and approval. The Component shall coordinate with the Contractor to ensure the letters meet the requirements of § 310.14.

(4) Subject to paragraph (a)(2) of this section, the Component shall inform the Deputy Secretary of Defense of the reasons why notice was not provided to the individuals or the affected population within the 10-day period.

(i) If for good cause (e.g., law enforcement authorities request delayed notification as immediate notification will jeopardize investigative efforts), notice can be delayed, but the delay shall only be for a reasonable period of time. In determining what constitutes a reasonable period of delay, the potential harm to the individual must be weighed against the necessity for delayed notification.

(ii) The required notification shall be prepared and forwarded to the Senior Component Official for Privacy who shall forward it to the Defense Privacy Office. The Defense Privacy Office, in coordination with the Office of the Under Secretary of Defense for Personnel and Readiness, shall forward the notice to the Deputy Secretary.

(5) The notice to the individual, at a minimum, shall include the following:

(i) The individuals shall be advised of what specific data was involved. It is insufficient to simply state that personal information has been lost. Where names, social security numbers, and dates of birth are involved, it is critical that the individual be advised that these data elements potentially have been compromised.

(ii) The individual shall be informed of the facts and circumstances surrounding the loss, theft, or compromise. The description of the loss should be sufficiently detailed so that the individual clearly understands how the compromise occurred.

(iii) The individual shall be informed of what protective actions the Component is taking or the individual can take to mitigate against potential future harm. The Component should refer the individual to the Federal Trade Commission's public Web site on identity theft at *http://www.consumer.gov/idtheft/con_steps.htm.* The site provides valuable information as to what steps individuals can take to protect themselves if their identities potentially have been or are stolen.

(iv) A sample notification letter is at appendix B.

(b) The notification shall be made whether or not the personal information is contained in a system of records (See § 310.10(a)).

Subpart C—Collecting Personal Information

§ 310.15 General considerations.

(a) *Collect directly from the individual.* Collect to the greatest extent practicable personal information directly from the individual to whom it pertains if the information may result in adverse determination about an individual's rights, privileges, or benefits under any Federal program.

(b) *Collecting social security numbers (SSNs).* (1) It is unlawful for any Federal, State, or local governmental agency to deny an individual any right, benefit, or privilege provided by law because the individual refuses to provide his or her SSN. However, if a Federal statute requires the SSN be furnished or if the SSN is furnished to a DoD Component maintaining a system of records in existence that was established and in operation before January 1, 1975, and the SSN was required under a statute or regulation adopted prior to this date for purposes of verifying the identity of an individual, this restriction does not apply.

(2) When an individual is requested to provide his or her SSN, he or she must be told:

(i) What uses will be made of the SSN;

(ii) The statute, regulation, or rule authorizing the solicitation of the SSN; and

(iii) Whether providing the SSN is voluntary or mandatory.

(3) Include in any systems notice for any system of records that contains SSNs a statement indicating the authority for maintaining the SSN.

(4) E.O. 9397,''Numbering System for Federal Accounts Relating to Individual Persons'', November 30, 1943, authorizes solicitation and use of SSNs as a numerical identifier for Federal personnel that are identified in most Federal record systems. However, it does not constitute authority for mandatory disclosure of the SSN.

(5) Upon entrance into military service or civilian employment with the Department of Defense, individuals are asked to provide their SSNs. The SSN becomes the service or employment number for the individual and is used to establish personnel, financial, medical, and other official records. The notification in paragraph (b)(2) of this section shall be provided the individual when originally soliciting his or her SSN. The notification is not required if an individual is requested to furnish his SSN for identification purposes and the SSN is solely used to verify the SSN that is contained in the records. However, if the SSN is solicited and retained for any purposes other than verifying the existing SSN in the records, the requesting official shall provide the individual the notification required by paragraph (b)(2) of this section.

(6) Components shall ensure that the SSN is only collected when there is a demonstrated need for collection. If collection is not essential for the purposes for which the record or records

are being maintained, it should not be solicited.

(7) DoD Components shall continually review their use of the SSN to determine whether such use can be eliminated, restricted, or concealed in Component business processes, systems and paper and electronic forms. While use of the SSN may be essential for program integrity and national security when information about an individual is disclosed outside the DoD, it may not be as critical when the information is being used for internal Departmental purposes.

(c) *Collecting personal information from third parties.* When information being solicited is of an objective nature and is not subject to being altered, the information should first be collected from the individual. But it may not be practicable to collect personal information first from the individual in all cases. Some examples of this are:

(1) Verification of information through third-party sources for security or employment suitability determinations;

(2) Seeking third-party opinions such as supervisor comments as to job knowledge, duty performance, or other opinion-type evaluations;

(3) When obtaining information first from the individual may impede rather than advance an investigative inquiry into the actions of the individual; and

(4) Contacting a third party at the request of the individual to furnish certain information such as exact periods of employment, termination dates, copies of records, or similar information.

(d) *Privacy Act Statements.* (1) When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, a Privacy Act Statement is required regardless of the medium used to collect the information (forms, personal interviews, telephonic interviews, or other methods). The Privacy Act Statement consists of the elements set forth in paragraph (d)(2)of this section. The statement enables the individual to make an informed decision whether to provide the information requested. If the personal information solicited is not to be incorporated into a system of records, the statement need not be given. However, personal information obtained without a Privacy Act Statement shall not be incorporated into any system of records. When soliciting SSNs for any purpose, see paragraph (b)(2) of this section.

(2) The Privacy Act Statement shall include:

(i) The Federal statute or Executive Order that authorizes collection of the requested information (See §310.10(d)).

(ii) The principal purpose or purposes for which the information is to be used;

(iii) The routine uses that will be made of the information (See §310.22(d));

(iv) Whether providing the information is voluntary or mandatory (See paragraph (e) of this section); and

(v) The effects on the individual if he or she chooses not to provide the requested information.

(3) The Privacy Act Statement shall be concise, current, and easily understood.

(4) The Privacy Act statement may appear as a public notice (sign or poster), conspicuously displayed in the area where the information is collected, such as at check-cashing facilities or identification photograph facilities (but see §310.16(a)).

(5) The individual normally is not required to sign the Privacy Act Statement.

(6) The individual shall be provided a written copy of the Privacy Act Statement upon request. This must be done regardless of the method chosen to furnish the initial advisement.

(e) *Mandatory as opposed to voluntary disclosures.* Include in the Privacy Act Statement specifically whether furnishing the requested personal data is mandatory or voluntary. A requirement to furnish personal data is mandatory only when the DoD Component is authorized to impose a penalty on the individual for failure to provide the requested information. If a penalty cannot be imposed, disclosing the information is always voluntary.

§310.16 Forms.

(a) *DoD Forms.* (1) DoD Instruction 7750.7[8] provides guidance for preparing Privacy Act Statements for use with

[8] See footnote 1 to §310.1.

forms (see also paragraph (b) of this section).

(2) When forms are used to collect personal information, the Privacy Act Statement shall appear as follows (listed in the order of preference):

(i) In the body of the form, preferably just below the title so that the reader will be advised of the contents of the statement before he or she begins to complete the form;

(ii) On the reverse side of the form with an appropriate annotation under the title giving its location;

(iii) On a tear-off sheet attached to the form; or

(iv) As a separate supplement to the form.

(b) *Forms issued by non-DoD activities.* (1) Forms subject to the Privacy Act issued by other Federal Agencies must have a Privacy Act Statement. Always ensure the statement prepared by the originating Agency is adequate for the purpose for which the form shall be used by the DoD activity. If the Privacy Act Statement provided is inadequate, the DoD Component concerned shall prepare a new statement or a supplement to the existing statement before using the form.

(2) Forms issued by agencies not subject to the Privacy Act (State, municipal, and other local agencies) do not contain Privacy Act Statements. Before using a form prepared by such agencies to collect personal data subject to this part, an appropriate Privacy Act Statement must be added.

Subpart D—Access by Individuals

§ 310.17 Individual access to personal information.

(a) *Individual access.* (1) The access provisions of this part are intended for use by individuals who seek access to records about themselves that are maintained in a system of records. Release of personal information to individuals under this part is not considered public release of the information.

(2) Make available to the individual to whom the record pertains all of the personal information contained in the system of records except where access may be denied pursuant to an exemption claimed for the system (see subpart F to this part). However, when the access provisions of this subpart are not available to the individual due to a claimed exemption, the request shall be processed to provide information that is disclosable pursuant to the DoD Freedom of Information Act program (see 32 CFR, part 286).

(b) *Individual requests for access.* Individuals shall address requests for access to personal information in a system of records to the system manager or to the office designated in the DoD Component procedural rules or the system notice.

(c) *Verification of identity.* (1) Before granting access to personal data, an individual may be required to provide reasonable proof of his or her identity.

(2) Identity verification procedures shall not:

(i) Be so complicated as to discourage unnecessarily individuals from seeking access to information about themselves; or

(ii) Be required of an individual seeking access to records that normally would be available under the DoD Freedom of Information Act Program (see 32 CFR, part 286).

(iii) When an individual seeks personal access to records pertaining to themselves in person, proof of identity is normally provided by documents that an individual ordinarily possesses, such as employee and military identification cards, driver's license, other licenses, permits or passes used for routine identification purposes.

(iv) When access is requested by mail, identity verification may consist of the individual providing certain minimum identifying data, such as full name, date and place of birth, or such other personal information necessary to locate the record sought and information that is ordinarily only known to the individual. If the information sought is of a sensitive nature, additional identifying data may be required. An unsworn declaration under penalty of perjury (28 U.S.C. 1746, ''Unsworn Declaration under Penalty of Perjury'') or notarized signatures are acceptable as a means of proving the identity of the individual.

(A) If an unsworn declaration is executed within the United States, its territories, possessions, or commonwealths, it shall read ''I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).''

(B) If an unsworn declaration is executed outside the United States, it shall read ''I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).''

(v) If an individual wishes to be accompanied by a third party when seeking access to his or her records or to have the records released directly to a third party, the individual may be required to furnish a signed access authorization granting the third-party access.

(vi) An individual shall not be refused access to his or her record solely because he or she refuses to divulge his or her SSN unless the SSN is the only method by which retrieval can be made. (See §310.15(b).)

(vii) The individual is not required to explain or justify his or her need for access to any record under this part.

(viii) Only a denial authority may deny access and the denial must be in writing and contain the information required by 310.18.

(d) *Granting individual access to records.* (1) Grant the individual access to the original record or an exact copy of the original record without any changes or deletions, except when deletions have been made in accordance with paragraph (e) of this Section. For the purpose of granting access, a record that has been amended under §310.19(b)is considered to be the original. See paragraph (e) of this Section for the policy regarding the use of summaries and extracts.

(2) Provide exact copies of the record when furnishing the individual copies of records under this part.

(3) Explain in terms understood by the requestor any record or portion of a record that is not clear.

(e) *Illegible, incomplete, or partially exempt records.* (1) Do not deny an individual access to a record or a copy of a record solely because the physical condition or format of the record does not make it readily available (for example, deteriorated state or on magnetic tape). Either prepare an extract or recopy the document exactly.

(2) If a portion of the record contains information that is exempt from access, an extract or summary containing all of the information in the record that is releasable shall be prepared.

(3) When the physical condition of the record or its state makes it necessary to prepare an extract for release, ensure the extract can be understood by the requester.

(4) Explain to the requester all deletions or changes to the records.

(f) *Access to medical records.* (1) Access to medical records is not only governed by the access provisions of this part but also by the access provisions of DoD 6025.18–R. The Privacy Act, as implemented by this part, however, provides greater access to an individual's medical record than that authorized by DoD 6025.18–R.

(2) Medical records in a system of records shall be disclosed to the individual to whom they pertain, even if a minor, but when it is believed that access to such records could have an adverse effect on the mental or physical health of the individual or may result in harm to a third party, the following special procedures apply.

(i) If a determination is made in consultation with a medical doctor that release of the medical information may be harmful to the mental or physical health of the individual or to a third party, the Component shall:

(A) Send the record to a physician named by the individual; and

(B) In the transmittal letter to the physician explain why access by the individual without proper professional supervision could be harmful (unless it is obvious from the record).

(ii) The Component shall not require the physician to request the records for the individual.

(3) If the individual refuses or fails to designate a physician, the record shall not be provided. Such refusal of access is not considered a denial under the Privacy Act (see paragraph (a) of §310.18).

(4) If records are provided the designated physician, but the physician declines or refuses to provide the records to the individual, the DoD Component is under an affirmative duty to take action to deliver the records to the individual by whatever means deemed appropriate. Such action should be taken expeditiously especially if there has been a significant delay between the time the records were furnished the physician and the decision by the physician not to release the records.

(5) Access to a minor's medical records may be granted to his or her parents or legal guardians. However, access is subject to the restrictions as set forth at paragraph C9.7.3 of DoD 6025.18–R.

(6) All members of the Military Services and all married persons are not considered minors regardless of age, and the parents of these individual do not have access to their medical records without written consent of the individual.

(g) *Access to information compiled in anticipation of civil action (see § 310.27).*

(h) *Non-Agency records.* (1) Certain documents under the physical control of DoD personnel and used to assist them in performing official functions, are not considered ''Agency records'' within the meaning of this part. Uncirculated personal notes and records that are not disseminated or circulated to any person or organization (for example, personal telephone lists or memory aids) that are retained or discarded at the author's discretion and over which the Component exercises no direct control are not considered Agency records. However, if personnel are officially directed or encouraged, either in writing or orally, to maintain such records, they may become ''Agency records,'' and may be subject to this part.

(2) The personal uncirculated handwritten notes of unit leaders, office supervisors, or military supervisory personnel concerning subordinates are not systems of records within the meaning of this part. Such notes are an extension of the individual's memory. These notes, however, must be maintained and discarded at the discretion of the individual supervisor and not circulated to others. Any established requirement to maintain such notes (such as, written or oral directives, regulations, or command policy) may transform these notes into ''Agency records'' and they then must be made a part of a system of records. If the notes are circulated, they must be made a part of a system of records. Any action that gives personal notes the appearance of official Agency records is prohibited, unless the notes have been incorporated into a system of records.

(i) *Relationship between the Privacy Act (5 U.S.C. 552a) and the FOIA (5 U.S.C. 552).* Not all requesters are knowledgeable of the appropriate statutory authority to cite when requesting records. In some instances, they may cite neither Act, but will imply one or both Acts. The below guidelines are provided to ensure requesters are given the maximum amount of information as authorized under both statutes. (1) Process requests for individual access as follows:

(i) If the records are required to be released under the Privacy Act, the FOIA (32 CFR part 286) does not bar release even if a FOIA exemption could be invoked if the request had been processed solely under FOIA. Conversely, if the records are required to be released under the FOIA, the Privacy Act does not bar disclosure.

(ii) Requesters who seek records about themselves contained in a Privacy Act system of records, and who cite or imply only the Privacy Act, will have their records processed under the provisions of this part and the FOIA (32 CFR part 286). If the system of records is exempt from the access provisions of this part, and if the records, or any portion thereof, are exempt under the FOIA, the requester shall be advised and informed of the appropriate Privacy and FOIA exemption. Only if the records can be denied under both statutes may the Department withhold the records from the individual. Appeals shall be processed under both Acts.

(iii) Requesters who seek records about themselves that are not contained in a Privacy Act system of records, and who cite or imply only the Privacy Act, will have their requests processed under the provisions of the FOIA (32 CFR part 286), because the access provisions of this part do not

apply. Appeals shall be processed under the FOIA.

(iv) Requesters who seek records about themselves that are contained in a Privacy Act system of records, and who cite or imply the FOIA or both Acts, will have their requests processed under the provisions of this part and the FOIA (32 CFR part 286). If the system of records is exempt from the access provisions of this part, and if the records, or any portion thereof, are exempt under the FOIA, the requester shall be advised and informed of the appropriate Privacy and FOIA exemption. Appeals shall be processed under both Acts.

(v) Requesters who seek records about themselves that are not contained in a Privacy Act system of records, and who cite or imply the Privacy Act and FOIA, will have their requests processed under the FOIA (32 CFR part 286), because the access provisions of this part do not apply. Appeals shall be processed under the FOIA.

(2) Do not deny individuals' access to personal information concerning themselves that would otherwise be releasable to them under either Act solely because they fail to cite or imply either Act or cite the wrong Act or part.

(3) Explain to the requester which Act(s) was(were) used when granting or denying access under either Act.

(j) *Time limits.* DoD Components normally shall acknowledge requests for access within 10 working days after receipt and provide access within 30 working days.

(k) *Privacy case file.* Establish a Privacy Act case file when required. (See paragraph (p) of §310.19.)

§310.18 Denial of individual access.

(a) *Denying individual access.* (1) An individual may be denied access to a record pertaining to him or her only if the record:

(i) Was compiled in reasonable anticipation of a civil action or proceeding (see §310.27).

(ii) Is in a system of records that has been exempted from the access provisions of this part under one of the permitted exemptions. (See §310.28 and §310.29.)

(iii) Contains classified information that has been exempted from the access provision of this part under the blanket exemption for such material claimed for all DoD records systems. (See §310.26(c).).

(iv) Is contained in a system of records for which access may be denied under some other Federal statute that excludes the record from coverage of the Privacy Act (5 U.S.C. 552a).

(2) Where a basis for denial exists, do not deny the record, or portions of the record, if denial does not serve a legitimate governmental purpose.

(b) *Other reasons to refuse access:*

(1) An individual may be refused access if:

(i) The record is not described well enough to enable it to be located with a reasonable amount of effort on the part of an employee familiar with the file; or

(ii) Access is sought by an individual who fails or refuses to comply with the established procedural requirements, including refusing to name a physician to receive medical records when required (see paragraph (f) of §310.17) or to pay fees (see §310.20).

(2) Always explain to the individual the specific reason access has been refused and how he or she may obtain access.

(c) *Notifying the individual.* Formal denials of access must be in writing and include as a minimum:

(1) The name, title or position, and signature of a designated Component denial authority.

(2) The date of the denial.

(3) The specific reason for the denial, including specific citation to the appropriate sections of the Privacy Act (5 U.S.C. 552a) or other statutes, this part, DoD Component instructions, or CFR authorizing the denial;

(4) Notice to the individual of his or her right to appeal the denial through the Component appeal procedure within 60 calendar days; and

(5) The title or position and address of the Privacy Act appeals official for the Component.

(d) *DoD Component appeal procedures.* Establish internal appeal procedures that, as a minimum, provide for:

(1) Review by the Head of the Component or his or her designee of any appeal by an individual from a denial of access to Component records.

(2) Formal written notification to the individual by the appeal authority that shall:

(i) If the denial is sustained totally or in part, include as a minimum:

(A) The exact reason for denying the appeal to include specific citation to the provisions of the Act or other statute, this part, Component instructions or the CFR upon which the determination is based;

(B) The date of the appeal determination;

(C) The name, title, and signature of the appeal authority; and

(D) A statement informing the applicant of his or her right to seek judicial relief.

(ii) If the appeal is granted, notify the individual and provide access to the material to which access has been granted.

(3) The written appeal notification granting or denying access is the final Component action as regards access.

(4) The individual shall file any appeal from denial of access within no less than 60 calendar days of receipt of the denial notification.

(5) Process all appeals within 30 days of receipt unless the appeal authority determines that a fair and equitable review cannot be made within that period. Notify the applicant in writing if additional time is required for the appellate review. The notification must include the reasons for the delay and state when the individual may expect an answer to the appeal.

(e) *Denial of appeals by failure to act.* A requester may consider his or her appeal formally denied if the appeal authority fails:

(1) To act on the appeal within 30 days;

(2) To provide the requester with a notice of extension within 30 days; or

(3) To act within the time limits established in the Component's notice of extension (see paragraph (d)(5) of this section).

(f) *Denying access to OPM records held by the DoD Components.* (1) The records in all systems of records maintained in accordance with the OPM Government-wide system notices are technically only in the temporary custody of the Department of Defense.

(2) All requests for access to these records must be processed in accordance with 5 CFR part 297 as well as applicable Component procedures.

(3) When a DoD Component refuses to grant access to a record in an OPM system, the Component shall advise the individual that his or her appeal must be directed to the Assistant Director for Workforce Information, Personnel Systems and Oversight Group, U.S. Office of Personnel Management, 1900 E Street, NW., Washington, DC, in accordance with the procedures of 5 CFR part 297.

§ 310.19 Amendment of records.

(a) *Individual review and correction.* Individuals are encouraged to review the personal information being maintained about them by the DoD Components periodically and to avail themselves of the procedures established by this part and other Regulations to update their records.

(b) *Amending records.* (1) An individual may request the amendment of any record contained in a system of records pertaining to him or her unless the system of records has been exempted specifically from the amendment procedures of this part under paragraph (b) of § 310.26. Normally, amendments under this part are limited to correcting factual matters and not matters of official judgment, such as performance ratings, promotion potential, and job performance appraisals.

(2) While a Component may require that the request for amendment be in writing, this requirement shall not be used to discourage individuals from requesting valid amendments or to burden needlessly the amendment process.

(3) A request for amendment must include:

(i) A description of the item or items to be amended;

(ii) The specific reason for the amendment;

(iii) The type of amendment action sought (deletion, correction, or addition); and

(iv) Copies of available documentary evidence supporting the request.

(c) *Burden of proof.* The applicant must support adequately his or her claim.

(d) *Identification of requesters.* (1) Individuals may be required to provide identification to ensure that they are indeed seeking to amend a record pertaining to themselves and not, inadvertently or intentionally, the record of others.

(2) The identification procedures shall not be used to discourage legitimate requests or to burden needlessly or delay the amendment process. (See paragraph (c) of § 310.17.)

(e) *Limits on attacking evidence previously submitted.* (1) The amendment process is not intended to permit the alteration of records presented in the course of judicial or quasi-judicial proceedings. Any amendments or changes to these records normally are made through the specific procedures established for the amendment of such records.

(2) Nothing in the amendment process is intended or designed to permit a collateral attack upon what has already been the subject of a judicial or quasi-judicial determination. However, while the individual may not attack the accuracy of the judicial or quasi-judicial determination under this part, he or she may challenge the accuracy of the recording of that action.

(f) *Sufficiency of a request to amend.* Consider the following factors when evaluating the sufficiency of a request to amend:

(1) The accuracy of the information; and

(2) The relevancy, timeliness, completeness, and necessity of the recorded information.

(g) *Time limits.* (1) Provide written acknowledgement of a request to amend within 10 working days of its receipt by the appropriate systems manager. There is no need to acknowledge a request if the action is completed within 10 working days and the individual is so informed.

(2) The letter of acknowledgement shall clearly identify the request and advise the individual when he or she may expect to be notified of the completed action.

(3) Only under the most exceptional circumstances shall more than 30 days be required to reach a decision on a request to amend. Document fully and explain in the Privacy Act case file (see paragraph (p) of this section) any such decision that takes more than 30 days to resolve.

(h) *Agreement to amend.* If the decision is made to grant all or part of the request for amendment, amend the record accordingly and notify the requester.

(i) *Notification of previous recipients.* (1) Notify all previous recipients of the record, as reflected in the disclosure accounting records, that an amendment has been made and the substance of the amendment. Recipients who are known to be no longer retaining the information need not be advised of the amendment. All DoD Components and Federal agencies known to be retaining the record or information, even if not reflected in a disclosure record, shall be notified of the amendment. Advise the requester of these notifications.

(2) Honor all requests by the requester to notify specific Federal agencies of the amendment action.

(j) *Denying amendment.* If the request for amendment is denied in whole or in part, promptly advise the individual in writing of the decision to include:

(1) The specific reason and authority for not amending;

(2) Notification that he or she may seek further independent review of the decision by the Head of the DoD Component or his or her designee;

(3) The procedures for appealing the decision citing the position and address of the official to whom the appeal shall be addressed; and

(4) Where he or she can receive assistance in filing the appeal.

(k) *DoD Component appeal procedures.* Establish procedures to ensure the prompt, complete, and independent review of each amendment denial upon appeal by the individual. These procedures must ensure:

(1) The appeal with all supporting materials both that furnished the individual and that contained in Component records is provided to the reviewing official; and

(2) If the appeal is denied completely or in part, the individual is notified in writing by the reviewing official that:

(i) The appeal has been denied and the specific reason and authority for the denial;

(ii) The individual may file a statement of disagreement with the appropriate authority and the procedures for filing this statement;

(iii) If filed properly, the statement of disagreement shall be included in the records, furnished to all future recipients of the records, and provided to all prior recipients of the disputed records who are known to hold the record; and

(iv) The individual may seek a judicial review of the decision not to amend.

(3) If the record is amended, ensure:

(i) The requester is notified promptly of the decision;

(ii) All prior known recipients of the records who are known to be retaining the record are notified of the decision and the specific nature of the amendment (see (l) of this section); and

(iii) The requester is notified which DoD Components and Federal agencies have been told of the amendment.

(4) Process all appeals within 30 days unless the appeal authority determines that a fair review cannot be made within this time limit. If additional time is required for the appeal, notify the requester, in writing, of the delay, the reason for the delay, and when he or she may expect a final decision on the appeal. Document fully all requirements for additional time in the Privacy Case File. (See paragraph (p) of this section.)

(l) *Denying amendment of OPM records held by the DoD Components.* (1) The records in all systems of records controlled by the OPM Government-wide system notices are technically only temporarily in the custody of the Department of Defense.

(2) All requests for amendment of these records must be processed in accordance with 5 CFR part 297. The Component denial authority may deny a request. However, when an amendment request is denied, the DoD Component shall advise the individual that his or her appeal must be directed to the Assistant Director for Workforce Information, Personnel Systems and Oversight Group, U.S. Office of Personnel Management, 1900 E Street, Washington, DC 20415 in accordance with the procedures of 5 CFR 297.

(m) *Statements of disagreement submitted by individuals.* (1) If the appellate authority refuses to amend the record as requested, the individual may submit a concise statement of disagreement setting forth his or her reasons for disagreeing with the decision not to amend.

(2) If an individual chooses to file a statement of disagreement, annotate the record to indicate that the statement has been filed (see paragraph (n) of this section).

(3) Furnish copies of the statement of disagreement to all DoD Components and Federal agencies that have been provided copies of the disputed information and who may be maintaining the information.

(n) *Maintaining statements of disagreement.* (1) When possible, incorporate the statement of disagreement into the record.

(2) If the statement cannot be made a part of the record, establish procedures to ensure that it is apparent from the records a statement of disagreement has been filed and maintain the statement so that it can be obtained readily when the disputed information is used or disclosed.

(3) Automated record systems that are not programmed to accept statements of disagreement shall be annotated or coded so they clearly indicate that a statement of disagreement is on file, and clearly identify the statement with the disputed information in the system.

(4) Provide a copy of the statement of disagreement whenever the disputed information is disclosed for any purpose.

(o) *The DoD Component statement of reasons for refusing to amend.* (1) A statement of reasons for refusing to amend may be included with any record for which a statement of disagreement is filed.

(2) Include in this statement only the reasons furnished to the individual for not amending the record. Do not comment on or respond to comments contained in the statement of disagreement. Normally, both statements are filed together.

(3) When disclosing information for which a statement of reasons has been filed, a copy of the statement may be released whenever the record and the statement of disagreement are disclosed.

(p) *Privacy case files.* (1) Establish a separate Privacy case file to retain the documentation received and generated during the amendment or access process.

(2) The Privacy case file shall contain as a minimum:

(i) The request for amendment and access.

(ii) Copies of the DoD Component's reply granting or denying the request;

(iii) Any appeals from the individual;

(iv) Copies of the action regarding the appeal with supporting documentation that is not in the basic file; and

(v) Any other correspondence generated in processing the appeal, to include coordination documentation.

(3) Only the items listed in paragraphs (p)(4) and (p)(5) of this section may be included in the system of records challenged for amendment or for which access is sought. Do not retain copies of the original record in the basic record system if the request for amendment is granted and the record has been amended.

(4) The following items relating to an amendment request may be included in the disputed record system:

(i) Copies of the amended record.

(ii) Copies of the individual's statement of disagreement (see paragraph (m) of this section).

(iii) Copies of the Component's statement of reasons for refusing to amend (see paragraph (o) of this section).

(iv) Supporting documentation submitted by the individual.

(5) The following items relating to an access request may be included in the basic records system:

(i) Copies of the request;

(ii) Copies of the Component's action granting total or partial access. (NOTE: A separate Privacy case file need not be created in such cases.)

(iii) Copies of the Component's action denying access.

(iv) Copies of any appeals filed.

(v) Copies of the reply to the appeal.

(6) Privacy case files shall not be furnished or disclosed to anyone for use in making any determination about the individual other than determinations made under this part.

§ 310.20 Reproduction fees.

(a) *Assessing fees.* (1) Charge the individual only the direct cost of reproduction.

(2) Do not charge reproduction fees if copying is:

(i) The only means to make the record available to the individual (for example, a copy of the record must be made to delete classified information); or

(ii) For the convenience of the DoD Component (for example, the Component has no reading room where an individual may review the record, or reproduction is done to keep the original in the Component's file).

(iii) No fees shall be charged when the record may be obtained without charge under any other Regulation, Directive, or statute.

(iv) Do not use fees to discourage requests.

(b) *No minimum fees authorized.* Use fees only to recoup direct reproduction costs associated with granting access. Minimum fees for duplication are not authorized and there is no automatic charge for processing a request.

(c) *Prohibited fees.* Do not charge or collect fees for:

(1) Search and retrieval of records;

(2) Review of records to determine releasability;

(3) Copying records for the DoD Component convenience or when the individual has not specifically requested a copy;

(4) Transportation of records and personnel; or

(5) Normal postage.

(d) *Waiver of fees.* (1) Normally, fees are waived automatically if the direct costs of a given request are less than $30. This fee waiver provision does not apply when a waiver has been granted to the individual before, and later requests appear to be an extension or duplication of that original request. A DoD Component may, however, set aside this automatic fee waiver provision when, on the basis of good evidence, it determines the waiver of fees is not in the public interest.

(2) Decisions to waive or reduce fees that exceed the automatic waiver threshold shall be made on a case-by-case basis.

(e) *Fees for members of Congress.* Do not charge members of Congress for copying records furnished even when the records are requested under the Privacy Act on behalf of a constituent (See § 310.22(i)). When replying to a constituent inquiry and the fees involved are substantial, consider suggesting to the Congressman that the constituent can obtain the information directly by writing to the appropriate offices and paying the costs. When practical, suggest to the Congressman that the record can be examined at no cost if the constituent wishes to visit the custodian of the record.

(f) *Reproduction fees computation.* Compute fees using the appropriate portions of the fee schedule in 32 CFR part 286.

Subpart E—Disclosure of Personal Information to Other Agencies and Third Parties

§ 310.21 Conditions of disclosure.

(a) *Disclosures to third parties.* (1) The Privacy Act only compels disclosure of records from a system of records to the individuals to whom they pertain unless the records are contained in a system for which an exemption to the access provisions of this part has been claimed.

(2) Requests by other individuals (third parties) for the records of individuals that are contained in a system of records shall be processed under 32 CFR part 286 except for requests by the parents of a minor or the legal guardian of an individual for access to the records pertaining to the minor or individual.

(b) *Disclosures among the DoD Components.* For the purposes of disclosure and disclosure accounting, the Department of Defense is considered a single agency (see § 310.22(a)).

(c) *Disclosures outside the Department of Defense.* Do not disclose personal information from a system of records outside the Department of Defense unless:

(1) The record has been requested by the individual to whom it pertains.

(2) The written consent of the individual to whom the record pertains has been obtained for release of the record to the requesting Agency, activity, or individual; or

(3) The release is authorized pursuant to one of the specific non-consensual conditions of disclosure as set forth in § 310.22.

(d) *Validation before disclosure.* Except for releases made in accordance with 32 CFR part 286, the following steps shall be taken before disclosing any records to any recipient outside the Department of Defense, other than a Federal agency or the individual to whom it pertains:

(1) Ensure the records are accurate, timely, complete, and relevant for agency purposes;

(2) Contact the individual, if reasonably available, to verify the accuracy, timeliness, completeness, and relevancy of the information, if this cannot be determined from the record; or

(3) If the information is not current and the individual is not reasonably available, advise the recipient that the information is believed accurate as of a specific date and any other known factors bearing on its accuracy and relevancy.

§ 310.22 Non-consensual conditions of disclosure.

(a) *Disclosures within the Department of Defense.* (1) Records pertaining to an individual may be disclosed to a DoD official or employee provided:

(i) The requester has a need for the record in the performance of his or her assigned duties. The requester shall articulate in sufficient detail why the records are required so the custodian of the records may make an informed decision regarding their release;

(ii) The intended use of the record generally relates to the purpose for which the record is maintained; and

(iii) Only those records as are minimally required to accomplish the intended use are disclosed. The entire record is not released if only a part of the record will be responsive to the request.

(2) Rank, position, or title alone does not authorize access to personal information about others.

(b) *Disclosures required by the FOIA.* (1) All records must be disclosed if their release is required by FOIA (5 U.S.C. 552), as implemented by 32 CFR part 286. The FOIA requires records be made available to the public unless withholding is authorized pursuant to one of nine exemptions or one of three law enforcement exclusions under the Act.

(i) The DoD Component must be in receipt of a FOIA request and a determination made that the records are not withholdable pursuant to a FOIA exemption or exclusion before the records may be disclosed.

(ii) Records that have traditionally been released to the public by the Components may be disclosed whether or not a FOIA request has been received.

(2) The standard for exempting most personal records, such as personnel, medical, and similar records, is FOIA Exemption 6 (32 CFR part 286.12(e)). Under that exemption, records can be withheld when disclosure, if other than to the individual about whom the information pertains, would result in a clearly unwarranted invasion of the individual's personal privacy.

(3) The standard for exempting personal records compiled for law enforcement purposes, including personnel security investigation records, is FOIA Exemption 7(C) (32 CFR part 286.12(g)). Under that exemption, records can be withheld when disclosure, if other than to the individual about whom the information pertains, would result in an unwarranted invasion of the individual's personal privacy.

(4) If records or information are exempt from disclosure pursuant to the standards set forth in paragraphs (b)(2) and/or (b)(3) of this section, and the records are contained in a system of records (See §310.10(a) of subpart B, the Privacy Act (5 U.S.C. 552a) prohibits release.

(5) *Personal information that is normally releasable*—(i) *DoD civilian employees.* (A) Some examples of personal information regarding DoD civilian employees that normally may be released without a clearly unwarranted invasion of personal privacy include:

(*1*) Name.

(*2*) Present and past position titles.

(*3*) Present and past grades.

(*4*) Present and past annual salary rates.

(*5*) Present and past duty stations.

(*6*) Office and duty telephone numbers.

(*7*) Position descriptions.

(B) All disclosures of personal information regarding Federal civilian employees shall be made in accordance with OPM release policies (see 5 CFR part 293.311).

(ii) *Military members.* (A) While it is not possible to identify categorically information that must be released or withheld from military personnel records in every instance, the following items of personal information regarding military members normally may be disclosed without a clearly unwarranted invasion of their personal privacy:

(*1*) Full name.

(*2*) Rank.

(*3*) Date of rank.

(*4*) Gross salary.

(*5*) Past duty assignments.

(*6*) Present duty assignment.

(*7*) Future assignments that are officially established.

(*8*) Office or duty telephone numbers.

(*9*) Source of commission.

(*10*) Promotion sequence number.

(*11*) Awards and decorations.

(*12*) Attendance at professional military schools.

(*13*) Duty status at any given time.

(*14*) Home of record (identification of the state only).

(*15*) Length of military service.

(*16*) Basic Pay Entry Date.

(*17*) Official Photo.

(B) All disclosures of personal information regarding military members shall be made in accordance with 32 CFR part 286.

(iii) *Civilian employees not under the authority of OPM.* (A) While it is not possible to identify categorically those items of personal information that must be released regarding civilian employees not subject to 5 CFR parts 293, 294, and 297, such as nonappropriated fund employees, normally the following items may be released without a clearly unwarranted invasion of personal privacy:

(*1*) Full name.

(*2*) Grade or position.

(*3*) Date of grade.

(*4*) Gross salary.

(*5*) Present and past assignments.

(*6*) Future assignments, if officially established.

(*7*) Office or duty telephone numbers.

(B) All releases of personal information regarding civilian personnel in this category shall be made in accordance with 32 CFR part 286.

(6) When military or civilian personnel are assigned, detailed, or employed by the National Security Agency, the Defense Intelligence Agency, the National Reconnaissance Office, or the National Geospatial-Intelligence agency, information about such personnel may only be disclosed as authorized by Public Law 86–36 (''National Security Agency-Officers and Employees'') and 10 U.S.C 424 (''Disclosure of Organizational and Personnel Information: Exemption for Specified Intelligence Agencies''). When military and civilian personnel are assigned, detailed or employed by an overseas unit, a sensitive unit, or to a routinely deployable unit, information about such personnel may only be disclosed as authorized by 10 U.S.C. 130b (''Personnel in Overseas, Sensitive, or Routinely Deployed Units: Nondisclosure of Personally Identifying Information'').

(7) Information about military or civilian personnel that otherwise may be disclosable consistent with §310.22(b)(5) may not be releasable if a requester seeks listings of personnel currently or recently assigned/detailed/employed within a particular component, unit, organization or office with the Department of Defense if the disclosure of such a list would pose a privacy or security threat.

(c) *Disclosures for established routine uses.* (1) Records may be disclosed outside the Department of Defense pursuant to a routine use that has been established for the system of records that contains the records.

(2) A routine use shall:

(i) Be compatible with the purpose for which the record was collected;

(ii) Identify the persons or organizations to whom the record may be released;

(iii) Identify specifically the intended uses of the information by the persons or organization; and

(iv) Have been published in the FEDERAL REGISTER (see §310.32(i)).

(3) If a Federal statute or an E.O. of the President directs records contained in a system of records be disclosed outside the Department of Defense, the statute or E.O. serves as authority for the establishment of a routine use.

(4) New or altered routine uses must be published in the FEDERAL REGISTER at least 30 days before any records may be disclosed pursuant to the terms of the routine use (see subpart G of this part).

(5) In addition to the specific routine uses established for each of the individual system notices, blanket routine uses have been established (see appendix 3) that are applicable to all DoD system of records. However, in order for the blanket routine uses to apply to a specific system of records, the system notice shall expressly state that the blanket routine uses apply. These blanket routine uses are published only at the beginning of the listing of system notices for each Component in the FEDERAL REGISTER.

(d) *Disclosures to the Bureau of the Census.* Records in DoD systems of records may be disclosed without the consent of the individuals to whom they pertain to the Bureau of the Census for purposes of planning or carrying out a census survey or related activities pursuant to the provisions of 13 U.S.C. 6 (''Information from other Federal Departments and Agencies'').

(e) *Disclosures for statistical research or reporting.* (1) Records may be disclosed for statistical research or reporting but only after the intended recipient provides, in writing, the purpose for which the records are sought and assurances that the records will be used only for statistical research or reporting purposes.

(2) The records shall be transferred to the requester in a form that is not individually identifiable. DoD Components disclosing records under this provision are required to assure information being disclosed cannot reasonably be used in any way to make determinations about individuals.

(3) The records will not be used, in whole or in part, to make any determination about the rights, benefits, or entitlements of specific individuals.

(4) The written statement by the requester shall be made part of the Component's accounting of disclosures (See paragraph (a) of 310.25).

(f) *Disclosures to the National Archives and Records Administration (NARA), General Services Administration (GSA).* (1) Records may be disclosed to the NARA if they:

(i) Have historical or other value to warrant continued preservation; or

(ii) For evaluation by the Archivist of the United States, or his or her designee, to determine if a record has such historical or other value.

(2) Records transferred to a Federal Records Center (FRC) for safekeeping and storage do not fall within this category. These records are owned by the Component and remain under the control of the transferring Component. FRC personnel are considered agents of the Component that retains control over the records. No disclosure accounting is required for the transfer of records to the FRCs.

(g) *Disclosures for law enforcement purposes.* (1) Records may be disclosed to another Agency or an instrumentality of any Governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity, provided:

(i) The civil or criminal law enforcement activity is authorized by law;

(ii) The head of the law enforcement activity or a designee has made a written request specifying the particular records desired and the law enforcement purpose (such as criminal investigations, enforcement of a civil law, or a similar purpose) for which the record is sought; and

(iii) There is no Federal statute that prohibits the disclosure of the records.

(2) Blanket requests for any and all records pertaining to an individual shall not be honored absent justification.

(3) When a record is released to a law enforcement activity under this subparagraph, the disclosure accounting (see § 310.25) for the release shall not be made available to the individual to whom the record pertains if the law enforcement activity requests that the disclosure not be disclosed.

(4) The blanket routine use for law enforcement (appendix C, section A) applies to all DoD Component systems notices (see paragraph (b)(6) of this section). This permits Components, on their own initiative, to report indications of violations of law found in a system of records to a law enforcement activity.

(5) Disclosures may be made to Federal, State, or local, but not foreign law enforcement agencies. Disclosures to Foreign law enforcement agencies may be made if a routine use has been established for the system of records from which the records are to be released.

(h) *Emergency disclosures.* (1) Records may be disclosed if disclosure is made under compelling circumstances affecting the health or safety of any individual. The affected individual need not be the subject of the record disclosed.

(2) When such a disclosure is made, the Component shall notify the individual who is the subject of the record. Notification sent to the last known address of the individual as known to the Component is sufficient.

(3) The specific data to be disclosed is at the discretion of the Component.

(4) Emergency medical information may be released by telephone.

(i) *Disclosures to Congress.* (1) Records may be disclosed to either House of the Congress or to any committee, joint committee or subcommittee of Congress if the release pertains to a matter within the jurisdiction of the committee. Disclosure is only authorized when in response to an official request on behalf of either House, committee, subcommittee, or joint committee.

(2) Requests from members of Congress who are seeking records in their individual capacity or on behalf of a constituent.

(i) Requests made in their individual capacity. Request for records shall be processed under the provisions of DoD 5400.7–R.

(ii) Requests made on behalf of constituents.

(A) The blanket routine use for ''Congressional Inquiries'' (see appendix C, section D) applies to all systems. When an individual requests the assistance of the Congressional member, the

blanket routine use permits the disclosure of records pertaining to the individual without the express written consent of the individual.

(B) If necessary, accept constituent letters requesting a member of Congress to investigate a matter pertaining to the individual as written authorization to provide access to the records to the congressional member or his or her staff.

(C) When a Congressional inquiry indicates that the request is being made on the basis of a request from the individual to whom the record pertains, consent can be inferred even if the constituent request is not provided the Component. The verbal statement by a Congressional staff member is acceptable to establish that a request has been received by the Member of Congress from the person to whom the records pertain.

(D) If the constituent inquiry is being made on behalf of someone other than the individual to whom the record pertains, the Member of Congress shall be provided only that information releasable under DoD 5400.7–R. Advise the Congressional member that the written consent of the individual to whom the record pertains is required before any additional information may be disclosed. Do not contact individuals to obtain their consents for release to Congressional members unless a Congressional office specifically requests that this be done.

(E) Nothing in paragraph (i)(2)(ii)(A) of this section prohibits a Component, when appropriate, from providing the record directly to the individual and notifying the Congressional office that this has been done without providing the record to the Congressional member.

(3) See paragraph (e) of § 310.20 for the policy on assessing fees for Members of Congress.

(4) Make a disclosure accounting each time a record is disclosed to either House of Congress, to any committee, joint committee, or subcommittee of Congress, or to any congressional member.

(j) *Disclosures to the General Accountability Office.* Records may be disclosed to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accountability Office.

(k) *Disclosures under court orders.* (1) Records may be disclosed without the consent of the person to whom they pertain under a court order signed by a judge of a court of competent jurisdiction.

(2) When a record is disclosed under this provision, make reasonable efforts to notify the individual to whom the record pertains, if the legal process is a matter of public record.

(3) If the process is not a matter of public record at the time it is issued, seek information as to when the process is to be made public and make reasonable efforts to notify the individual at that time.

(4) Notification sent to the last known address of the individual as reflected in the records is considered a reasonable effort to notify.

(5) Make a disclosure accounting each time a record is disclosed under a court order or compulsory legal process.

(l) *Disclosures to consumer reporting agencies.* (1) Certain personal information may be disclosed to consumer reporting agencies as provided in the Federal Claims Collection Act (31 U.S.C. 3711(e)).

(2) Under the provisions of paragraph (l)(1) of this section, the following information may be disclosed to a consumer reporting agency:

(i) Name, address, taxpayer identification number (SSN), and other information necessary to establish the identity of the individual.

(ii) The amount, status, and history of the claim.

(iii) The Agency or program under which the claim arose.

(3) The Federal Claims Collection Act (31 U.S.C. 3711(e)) requires the system notice for the system of records from which the information will be disclosed, indicates that the information may be disclosed to a consumer reporting agency.

§ 310.23 Disclosures to commercial enterprises.

(a) *General policy.* (1) Make releases of personal information to commercial enterprises under the criteria established by 32 CFR part 286.

(2) The relationship of commercial enterprises to their clients or customers and to the Department of Defense is not changed by this part.

(3) The DoD policy on personal indebtedness for military personnel is contained 32 CFR part 112, ''Indebtedness of Military Personnel,'' and for civilian employees in 5 CFR part 735.

(b) *Release of personal information.* (1) Any information that must be released under 32 CFR part 286, the ''DoD Freedom of Information Act Program,'' may be released to a commercial enterprise without the individual's consent (see paragraph (b) of § 310.22).

(2) Commercial enterprises may present a signed consent statement setting forth specific conditions for release of personal information. Statements such as the following, if signed by the individual, are considered valid:

I hereby authorize the Department of Defense to verify my Social Security Number or other identifying information and to disclose my home address and telephone number to authorized representatives of (name of commercial enterprise) so that they may use this information in connection with my commercial dealings with that enterprise. All information furnished shall be used in connection with my financial relationship with (name of commercial enterprise).

(3) When a statement of consent as outlined in paragraph (b)(2) of this section is presented, provide the requested information if its release is not prohibited by some other regulation or statute.

(4) Blanket statements of consent that do not identify the Department of Defense or any of its Components, or that do not specify exactly the type of information to be released, may be honored if it is clear the individual in signing the consent statement intended to obtain a personal benefit (for example, a loan to buy a house) and was aware of the type of information that would be sought. Care should be exercised in these situations to release only the minimum amount of personal information essential to obtain the benefit sought.

(5) Do not honor requests from commercial enterprises for official evaluation of personal characteristics, such as evaluation of personal financial habits.

§ 310.24 Disclosures to the public from medical records.

(a) Disclosures from medical records are not only governed by the requirement of this part but also by the disclosure provisions of DoD 6025.18–R.''

(b) Any medical records that are subject to both this part and DoD 6025.18–R may only be disclosed if disclosure is authorized under both. If disclosure is permitted under this part (e.g., pursuant to a routine use), but the disclosure is not authorized under DoD 6025.18-R, disclosure is not authorized. If a disclosure is authorized under DoD 6025.18–R (e.g., releases outside the Department of Defense), but the disclosure is not authorized under this part, disclosure is not authorized.

§ 310.25 Disclosure accounting.

(a) *Disclosure accountings.* (1) Keep an accurate record of all disclosures made from any system of records except disclosures:

(i) To DoD personnel for use in the performance of their official duties; or

(ii) Under 5 U.S.C. 552, the FOIA.

(2) In all other cases a disclosure accounting is required even if the individual has consented to the disclosure of the information.

(3) Disclosure accountings:

(i) Permit individuals to determine to whom information has been disclosed;

(ii) Enable the activity to notify past recipients of disputed or corrected information (§ 310.19(i)); and

(iii) Provide a method of determining compliance with paragraph (c) of § 310.21.

(b) *Contents of disclosure accountings.* As a minimum, disclosure accounting shall contain:

(1) The date of the disclosure.

(2) A description of the information released.

(3) The purpose of the disclosure.

(4) The name and address of the person or Agency to whom the disclosure was made.

(c) *Methods of disclosure accounting.* Use any system of disclosure accounting that shall provide readily the necessary disclosure information (see paragraph (a)(3) of this section).

(d) *Accounting for mass disclosures.* When numerous similar records are released, identify the category of records disclosed and include the data required by paragraph (b) of this section in a form that can be used to construct an accounting disclosure record for individual records if required (see paragraph (a)(3) of this section).

(e) *Disposition of disclosure accounting records.* Retain disclosure accounting records for 5 years after the disclosure or the life of the record, whichever is longer.

(f) *Furnishing disclosure accountings to the individual.* (1) Make available to the individual to whom the record pertains all disclosure accountings except when:

(i) The disclosure has been made to a law enforcement activity under paragraph (g) of § 310.22 and the law enforcement activity has requested that disclosure not be made; or

(ii) The system of records has been exempted from the requirement to furnish the disclosure accounting under the provisions of § 310.26(b).

(2) If disclosure accountings are not maintained with the record and the individual requests access to the accounting, prepare a listing of all disclosures (see paragraph (b) of this section) and provide this to the individual upon request.

Subpart F—Exemptions

§ 310.26 Use and establishment of exemptions.

(a) *Types of exemptions.* (1) There are three types of exemptions permitted by the Privacy Act (5 U.S.C. 552a).

(i) An access exemption that exempts records compiled in reasonable anticipation of a civil action or proceeding from the access provisions of the Act.

(ii) General exemptions that authorize the exemption of a system of records from all but certain specifically identified provisions of the Act (see appendix D).

(iii) Specific exemptions that allow a system of records to be exempted only from certain designated provisions of the Act (see appendix D).

(2) Nothing in the Act permits exemption of any system of records from all provisions of the Act.

(b) *Establishing exemptions.* (1) The access exemption is self-executing. It does not require an implementing rule to be effective.

(2) Neither a general nor a specific exemption is established automatically for any system of records. The Heads of the DoD Components maintaining the system of records must make a determination whether the system is one for which an exemption properly may be claimed and then propose and establish an exemption rule for the system. No system of records within the Department of Defense shall be considered exempted until the Head of the Component has approved the exemption and an exemption rule has been published as a final rule in the FEDERAL REGISTER (See § 310.30(e).)

(3) Only the Head of the DoD Component or an authorized designee may claim an exemption for a system of records.

(4) A system of records is considered exempt only from those provision of the Privacy Act (5 U.S.C. 552a) that are identified specifically in the Component exemption rule for the system and that are authorized by the Privacy Act.

(5) To establish an exemption rule, see § 310.31.

(c) *Blanket exemption for classified material.* (1) Component rules shall include a blanket exemption under 5 U.S.C. 552a(k)(1) of the Privacy Act from the access provisions (5 U.S.C. 552a(d)) and the notification of access procedures (5 U.S.C. 522a(e)(4)(H)) of the Act for all classified material in any systems of records maintained.

(2) Do not claim specifically an exemption under section 552a(k)(1) of the Privacy Act for any system of records. The blanket exemption affords protection to all classified material in all system of records maintained.

(d) *Provisions from which exemptions may be claimed.* The Head of a DoD Component may claim an exemption from any provision of the Act from which an exemption is allowed (see appendix D).

(e) *Use of exemptions.* (1) Use exemptions only for the specific purposes set forth in the exemption rules (see paragraph (b) of § 310.31).

(2) Use exemptions only when they are in the best interest of the Government and limit them to the specific portions of the records requiring protection.

(3) Do not use an exemption to deny an individual access to any record to which he or she would have access under 32 CFR part 286.

(f) *Exempt records in non-exempt systems.* (1) Exempt records temporarily in the custody of another Component are considered the property of the originating Component. Access to these records is controlled by the system notices and rules of the originating Component.

(2) Exempt records that have been incorporated into a nonexempt system of records are still exempt but only to the extent to which the provisions of the Act for which an exemption has been claimed are identified and an exemption claimed for the system of records from which the record is obtained and only when the purposes underlying the exemption for the record are still valid and necessary to protect the contents of the record.

(3) If a record is accidentally misfiled into a system of records, the system notice and rules for the system in which it should actually be filed shall govern.

§ 310.27 Access exemption.

(a) An individual is not entitled to access information that is compiled in reasonable anticipation of a civil action or proceeding.

(b) The term ''civil action or proceeding'' is intended to include court proceedings, preliminary judicial steps, and quasi-judicial administrative hearings or proceedings (i.e., adversarial proceedings that are subject to rules of evidence).

(c) Any information prepared in anticipation of such actions or proceedings, to include information prepared to advise the DoD Component officials of the possible legal or other consequences of a given course of action, is protected.

(d) The exemption is similar to the attorney work-product privilege except that it applies even when the information is prepared by nonattorneys.

(e) The exemption does not apply to information compiled in anticipation of criminal actions or proceedings.

§ 310.28 General exemption.

(a) *Use of specific exemptions.* A DoD Component is not authorized to claim the exemption for records maintained by the Central Intelligence Agency established by 5 U.S.C. 552a(j)(1) of the Privacy Act.

(b) The general exemption established by 5 U.S.C. 552a(j)(2) of the Privacy Act may be claimed to protect investigative records created and maintained by law-enforcement activities of a DoD Component.

(c) To qualify for the (j)(2) exemption, the system of records must be maintained by a DoD Component, or element thereof, that performs as its principal function any activity pertaining to the enforcement of criminal laws, such as the U.S. Army Criminal Investigation Command, the Naval Investigative Service, the Air Force Office of Special Investigations, and military police activities. However, where DoD offices perform multiple functions, but have an investigative component, such as the DoD Inspector General Defense Criminal Investigative Service or Criminal Law Divisions of Staff Judge Advocates Offices, the exemption may be claimed. Law enforcement includes police efforts to detect, prevent, control, or reduce crime, to apprehend or identify criminals; and the activities of military trial counsel, correction, probation, pardon, or parole authorities.

(d) Information that may be protected under the (j)(2) exemption includes:

(1) Records compiled for the purpose of identifying criminal offenders and alleged offenders consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, parole, and probation status (so-called criminal history records);

(2) Reports and other records compiled during criminal investigations, including supporting documentation.

(3) Other records compiled at any stage of the criminal law enforcement process from arrest or indictment

through the final release from parole supervision, such as pre-sentence and parole reports.

(e) The (j)(2) exemption does not apply to:

(1) Investigative records prepared or maintained by activities without primary law-enforcement missions. It may not be claimed by any activity that does not have law enforcement as its principal function except as indicated in paragraph (c) of this section.

(2) Investigative records compiled by any activity concerning employee suitability, eligibility, qualification, or for individual access to classified material regardless of the principal mission of the compiling DoD Component.

§ 310.29 Specific exemptions.

(a) *Use of specific exemptions.* The specific exemption established by 5 U.S.C. 552a(k) of the Privacy Act may be claimed to protect records that meet the following criteria (parenthetical references are to the appropriate subsection of the Act:

(1) *(k)(1).* Information subject to 5 U.S.C. 552(b)(1), (DoD 5200.1-R) (see also paragraph (c) of this section).

(2) *(k)(2).* Investigatory information compiled for law-enforcement purposes, other than information that is covered by the general exemption (see § 310.28). If an individual is denied any right, privilege or benefit he or she is otherwise entitled by Federal law or for which he or she would otherwise be eligible as a result of the maintenance of the information, the individual shall be provided access to the information except to the extent that disclosure would reveal the identity of a confidential source. This exemption provides limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(i) The information must be compiled for some investigative law enforcement purpose, such as a criminal investigation by a DoD office, whose principal function is not law enforcement, or a civil investigation.

(ii) The exemption does not apply to investigations conducted solely for the purpose of a routine background investigation (see paragraph (a)(5) of this section), but will apply if the investigation is for the purpose of investigating DoD personnel who are suspected of violating statutory or regulatory authority.

(iii) The exemption can continue to be claimed even after the investigation has concluded and there is no future likelihood of further enforcement proceedings.

(3) *(k)(3).* Records maintained in connection with providing protective services to the President and other individuals under 18 U.S.C. 3056, ''Powers, Authorities, and Duties of United States Secret Service.''

(4) *(k)(4).* Records maintained solely for statistical research or program evaluation purposes and that are not used to make decisions on the rights, benefits, or entitlement of an individual except for census records that may be disclosed under 13 U.S.C. 6, ''Information for other Federal Departments and Agencies.

(5) *(k)(5).* Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent such material would reveal the identity of a confidential source.

(i) This exemption permits protection of confidential sources used in background investigations, employment inquiries, and similar inquiries that are for personnel screening to determine suitability, eligibility, or qualifications.

(ii) This exemption is applicable not only to investigations conducted prior to the hiring of an employee, but it also applies to investigations conducted to determine continued employment suitability or eligibility.

(6) *(k)(6).* Testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal or military service, if the disclosure would compromise the objectivity or fairness of the test or examination process.

(7) *(k)(7).* Evaluation material used to determine potential for promotion in the Military Services, but only to the extent that the disclosure of such material would reveal the identity of a confidential source.

(b) *Promises of confidentiality.* (1) Only the identity of sources that have been given an express promise of confidentiality may be protected from disclosure under paragraphs (a)(1), (5), and (7) of this section. However, the identity of sources who were given implied promises of confidentiality in inquiries conducted before September 27, 1975, also may be protected from disclosure.

(2) Ensure promises of confidentiality are not automatically given but are used sparingly. Establish appropriate procedures and identify fully categories of individuals who may make such promises. Promises of confidentiality shall be made only when they are essential to obtain the information sought (see 5 CFR part 736).

(c) *Access to records for which specific exemptions are claimed.* Deny the individual access only to those portions of the records for which the claimed exemption applies.

Subpart G—Publication Requirements

§ 310.30 Federal Register publication.

(a) *What must be published in the* FEDERAL REGISTER. (1) Four types of documents relating to the Privacy Program must be published in the FEDERAL REGISTER:

(i) DoD Component Privacy Procedural rules;

(ii) DoD Component exemption rules; and

(iii) System notices.

(iv) Match notices (See subpart L to this part).

(2) See DoD 5025.1–M,[9] ''Directive Systems Procedures'' and Administrative Instruction (AI) No. 102,[10] ''Office of the Secretary of Defense Federal Register System'' for information pertaining to the preparation of documents for publication in the FEDERAL REGISTER.

(b) *The effect of publication in the* FEDERAL REGISTER. Publication of a document in the FEDERAL REGISTER constitutes official public notice of the existence and content of the document.

(c) *DoD Component rules.* (1) Component Privacy Program procedures and Component exemption rules are subject to the rulemaking procedures prescribed in AI 102.

(2) System notices are not subject to formal rulemaking and are published in the FEDERAL REGISTER as ''Notices,'' not rules.

(3) Privacy procedural and exemption rules are incorporated automatically into the CFR. System notices are not published in the CFR.

(d) *Submission of rules for publication.* (1) Submit to the DPO, ODA&M, all proposed rules implementing this part in proper format (see DoD 5025.1–M and AI 102) for publication in the FEDERAL REGISTER.

(2) This part has been published as a final rule in the FEDERAL REGISTER. Therefore, incorporate it into your Component rules rather than by republication (see AI 102).

(3) DoD Component procedural rules that simply implement this Regulation need only be published as final rules in the FEDERAL REGISTER (see DoD 5025.1–M and AI 102). If the Component procedural rule supplements this part in any manner, they must be published as a proposed rule before being published as a final rule.

(4) Amendments to Component rules are submitted like the basic rules.

(5) The DPO submits the rules and amendments thereto to the FEDERAL REGISTER for publication.

(e) *Submission of exemption rules for publication.* (1) No system of records within the Department of Defense shall be considered exempt from any provision of this part until the exemption and the exemption rule for the system has been published as a final rule in the FEDERAL REGISTER.

(2) Submit exemption rules in proper format to the DPO. All exemption rules are coordinated with the DoD Office of General Counsel. After coordination, the DPO shall submit the rules to the FEDERAL REGISTER for publication.

(3) Exemption rules require publication both as proposed rules and final rules (see AI 102).

(4) § 310.31(b) discusses the content of an exemption rule.

(5) Submit amendments to exemption rules in the same manner used for establishing these rules.

[9] See footnote 1 to § 310.1.

[10] See footnote 1 to § 310.1.

(f) *Submission of system notices for publication.* (1) System notices are not subject to formal rulemaking procedures. However, the Privacy Act (5 U.S.C. 552a) requires a system notice be published in the FEDERAL REGISTER of the existence and character of a new or altered system of records. Until publication of the notice, DoD Components shall not begin to operate the system of records (i.e., collect and use the information). The notice procedures require:

(i) The system notice describes what kinds of records are in the system, on whom they are maintained, what uses are made of the records, and how an individual may access, or contest, the records contained in the system.

(ii) The public be given 30 days to comment on any proposed routine uses before any disclosures are made pursuant to the routine use; and

(iii) The notice contain the date on which the system shall become effective.

(2) Submit system notices to the DPO in the FEDERAL REGISTER format (see AI 102 and appendix E to this part). The DPO transmits the notices to the FEDERAL REGISTER for publication.

(3) § 310.32 discusses the specific elements required in a system notice.

§ 310.31 Exemption rules.

(a) *General procedures.* Subpart F of this part provides the general guidance for establishing exemptions for systems of records.

(b) *Contents of exemption rules.* (1) Each exemption rule submitted for publication must contain the following:

(i) The record system identifier and title of the system for which the exemption is claimed. (See § 310.32(b) and (c));

(ii) The specific sections of the Privacy Act under which the exemption for the system is claimed (for example, 5 U.S.C. 552a(j)(2), 5 U.S.C. 552a(k)(3); or 5 U.S.C. 552a(k)(7);

(iii) The specific sections of the Privacy Act from which the system is to be exempted (for example, 5 U.S.C. 552a(c)(3), or 5 U.S.C. 552a(d)(l)–(5)) (see appendix D)); and

(iv) The specific reasons why an exemption is being claimed from each section of the Act identified.

(2) Do not claim an exemption for classified material for individual systems of records. The blanket exemption applies. (See paragraph (c) of § 310.26.)

§ 310.32 System notices.

(a) *Contents of the system notices.* (1) The following data captions are included in each system notice:

(i) Systems identifier. (see paragraph (b) of this section).

(ii) System name. (see paragraph (c) of this section).

(iii) System location. (see paragraph (d) of this section).

(iv) Categories of individuals covered by the system. (see paragraph (e) of this section).

(v) Categories of records in the system. (see paragraph (f) of this section).

(vi) Authority for maintenance of the system. (see paragraph (g) of this section).

(vii) Purpose(s). (see paragraph (h) of this section).

(viii) Routine uses of records maintained in the system, including categories of users and the purposes of such uses. (see paragraph (i) of this section).

(ix) Disclosure to Consumer Reporting Agencies. This element is optional but required when disclosing to consumer reporting agencies (See paragraph (l) of § 310.22.)

(x) Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system. (see paragraph (j) of this section).

(xi) Systems manager(s) and address. (see paragraph (k) of this section).

(xii) Notification procedure. (see paragraph (l) of this section).

(xiii) Record access procedures. (see paragraph (m) of this section).

(xiv) Contesting records procedures. (see paragraph (n) of this section).

(xv) Record source categories. (see paragraph (o) of this section).

(xvi) Exemptions claimed for the system. (see paragraph (p) of this section).

(2) The captions listed in paragraph (a)(1) of this Section have been mandated by the Office of Federal Register and must be used exactly as presented.

(3) A sample system notice is shown in appendix E of this part.

(b) *System identifier.* The system identifier must appear on all system notices and is limited to 21 positions, unless an exception is granted by the DPO, including Component code, file number and symbols, punctuation, and spacing.

(c) *System name.* (1) The name of the system reasonably identifies the general purpose of the system and, if possible, the general categories of individuals involved.

(2) Use acronyms only parenthetically following the title or any portion thereof, such as, ''Joint Uniform Military Pay System (JUMPS).'' Do not use acronyms not commonly known unless they are preceded by an explanation.

(3) The system name may not exceed 55 character positions, unless an exception is granted by the DPO, including punctuation and spacing.

(4) The system name should not be the name of the database or the IT system if the name does not meet the criteria in paragraph (c)(1) of this section.

(d) *System location.* (1) For systems maintained in a single location provide the exact office name, organizational identity, and address.

(2) For geographically or organizationally decentralized systems, specify each level of organization or element that maintains a segment of the system, to include their mailing address, or indicate the official mailing addresses are published as an Appendix to the Component's compilation of system of records notices, or provide an address where a complete listing of locations can be obtained.

(3) Use the standard U.S. Postal Service two-letter State abbreviation symbols and 9-digit Zip Codes for all domestic addresses.

(e) *Categories of individuals covered by the system.* (1) Set forth the specific categories of individuals to whom records in the system pertain in clear, easily understood, non-technical terms.

(2) Avoid the use of broad over-general descriptions, such as ''all Army personnel'' or ''all military personnel'' unless this actually reflects the category of individuals involved.

(f) *Categories of records in the system.* (1) Describe in clear, non-technical terms the types of records maintained in the system.

(2) Only documents actually maintained in the system of records shall be described, not source documents that are used only to collect data and then destroyed.

(g) *Authority for maintenance of system.* (1) Cite the specific provision of the Federal statute or E.O. that authorizes the maintenance of the system.

(2) Include with citations for statutes the popular names, when appropriate (for example, Section 2103 of title 51, United States Code, ''Tea-Tasters Licensing Act''), and for E.O.s, the official title (for example, E.O. No. 9397, ''Numbering System for Federal Accounts Relating to Individual Persons'').

(3) If direct statutory authority or an Executive Order does not exist, indirect statutory authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(4) If direct or indirect authority does not exist, the Department of Defense, as well as the Army, Navy, and Air Force general ''housekeeping'' statutes (i.e., 5 U.S.C. 301 (''Departmental Regulations''), 10 U.S.C. 3013 (''Secretary of the Army''), 5013 (''Secretary of the Navy''), and 8013 (''Secretary of the Air Force'') may be cited if the Secretary, or those offices to which responsibility has been delegated, are required to collect and maintain systems of records in order to discharge assigned responsibilities. If the housekeeping statute is cited, the regulatory authority implementing the statute within the Department or Component also shall be identified.

(5) If the social security number is being collected and maintained, E.O. 9397 (''Numbering Systems for Federal Accounts Relating to Indivdiual Persons'') shall be cited.

(h) *Purpose or Purposes.* (1) List the specific purposes for maintaining the system of records by the Component.

(2) All internal uses of the information within the Department or Component shall be identified. Such uses are the so-called ''internal routine uses.''

(i) *Routine uses.* (1) Except as otherwise authorized by subpart E of this part, disclosure of information from a system of records to any person or entity outside the Department of Defense (see §310.21(b)) may only be made pursuant to a routine use that has been established for the specific system of records. Such uses are the so-called ''external routine uses.''

(2) Each routine use shall include to whom the information is being disclosed and what use and purpose the information will be used. Routine uses shall be written as follows:

(i) ''To* * *.[person or entity outside of DoD that will receive the information] to* * *.[what will be done with the information] for the purpose(s) of * * *[what objective is sought to be achieved].''

(ii) To the extent practicable, general statements, such as ''to other Federal agencies as required'' or ''to any other appropriate Federal agency'' shall be avoided.

(3) Blanket routine uses (appendix C to this part) have been adopted that apply to all Component system notices. The blanket routine uses appear at the beginning of each Component's compilation of its system notices.

(i) Each system notice shall contain a statement whether or not the blanket routine uses apply to the system.

(ii) Each notice may state that none of the blanket routine uses apply or that one or more do not apply.

(j) *Policies and practices for storing, retiring, accessing, retaining, and disposing of records.* This caption is subdivided into four parts:

(1) *Storage.* Indicate the medium in which the records are maintained. (For example, a system may be ''automated, maintained on compact disks, diskettes,'' ''manual, maintained in paper files,'' or ''hybrid, maintained in a combination of paper and automated form.'') Storage does not refer to the container or facility in which the records are kept.

(2) *Retrievability.* Specify how the records are retrieved (for example, name, SSN, or some other unique personal identifier assigned the individual).

(3) *Safeguards.* Identify the system safeguards (such as storage in safes, vaults, locked cabinets or rooms, use of guards, visitor registers, personnel screening, or password protected IT systems). Also identify personnel who have access to the systems. Do not describe safeguards in such detail as to compromise system security.

(4) *Retention and disposal.* Indicate how long the record is retained. When appropriate, also state the length of time the records are maintained by the Component, when they are transferred to a FRC, time of retention at the Records Center and when they are transferred to the National Archivist or are destroyed. A reference to a Component regulation without further detailed information is insufficient. If records are eventually destroyed as opposed to being retired, identify the method of destruction (e.g., shredding, burning, pulping, etc).

(k) *System manager or managers and address.* (1) List the title and address of the official responsible for the management of the system.

(2) If the title of the specific official is unknown, such as for a local system, specify the local commander or office head as the systems manager.

(3) For geographically separated or organizationally decentralized activities for which individuals may deal directly with officials at each location in exercising their rights, list the position or duty title of each category of officials responsible for the system or a segment thereof.

(4) Do not include business or duty addresses if they are listed in the Component address directory.

(l) *Notification procedures.* (1) Describe how an individual may determine if there are records pertaining to him or her in the system. The procedural rules may be cited, but include a brief procedural description of the needed data. Provide sufficient information in the notice to allow an individual to exercise his or her rights without referral to the formal rules.

(2) As a minimum, the caption shall include:

(i) The official title (normally the system manager) and official address to which the request is to be directed.

(ii) The specific information required to determine if there is a record of the individual in the system.

(iii) Identification of the offices through which the individual may obtain notification; and

(iv) A description of any proof of identity required. (see §310.17(c)).

(3) When appropriate, the individual may be referred to a Component official who shall provide this information to him or her.

(m) *Record access procedures.* (1) Describe how an individual can gain access to the records pertaining to him or her in the system. The procedural rules may be cited, but include a brief procedural description of the needed data. Provide sufficient information in the notice to allow an individual to exercise his or her rights without referral to the formal rules.

(2) As a minimum, the caption shall include:

(i) The official title (normally the system manager) and official address to which the request is to be directed.

(ii) A description of any proof of identity required. (see §310.17(c)).

(iii) When appropriate, the individual may be referred to a Component official who shall provide the records to him or her.

(n) *Contesting record procedures.* (1) Describe how an individual may contest the content of a record pertaining to him or her in the system.

(2) The detailed procedures for contesting a record need not be identified if the Component procedural rules are readily available to the public. (For example, ''The Office of the Secretary of Defense'' rules for contesting contents are contained in 32 CFR 311.) All Component procedural rules are set forth at a Departmental public Web site (*http://www.defenselink.mil/privacy/cfr-rules.html*).

(3) The individual may also be referred to the system manager to determine these procedures.

(o) *Record source categories.* (1) Describe where (the individual, other Component documentation, other Federal agencies, etc) the information contained in the system was obtained.

(2) Specific individuals or institutions need not be identified by name, particularly if these sources have been granted confidentiality. (see §310.29(b)).

(p) *Exemptions claimed for the System.* (1) If no exemption has been claimed for the system, indicate ''None.''

(2) If an exemption is claimed, cite the exemption as well as identifying the CFR section containing the exemption rule for the system.

(q) *Maintaining the Master DoD System Notice Registry.* (1) The DPO maintains a master registry of all DoD record systems notices.

(2) The DPO also posts all DoD system notices to a public Web site (see *http://www.defenselink.mil/privacy/notices*).

§310.33 New and altered record systems.

(a) *Criteria for a new record system.* (1) If a Component is maintaining a system of records as contemplated by §310.10(a), and a system notice has not been published for it in the FEDERAL REGISTER, the Component shall establish a system notice consistent with the requirements of this subpart.

(2) If a notice for a system of records has been canceled or deleted but a determination is subsequently made that the system will be reinstated or reused, the system may not be operated (i.e., information collected or used) until a new notice is published in the FEDERAL REGISTER.

(b) *Criteria for an altered record system.* A system is considered altered whenever one of the following actions occurs or is proposed:

(1) A significant increase or change in the number or type of individuals about whom records are maintained.

(i) Only changes that alter significantly the character and purpose of the record system are considered alterations.

(ii) Increases in numbers of individuals due to normal growth are not considered alterations unless they truly alter the character and purpose of the system.

(iii) Increases that change significantly the scope of population covered (for example, expansion of a system of records covering a single command's enlisted personnel to include all of the

Component's enlisted personnel would be considered an alteration).

(iv) A reduction in the number of individuals covered is not an alteration, but only an amendment. (see § 310.34(a).)

(v) All changes that add new categories of individuals to system coverage require a change to the ''Categories of individuals covered by the system'' caption of the notice (see § 310.32(e)) and may require changes to the ''Purpose(s)'' caption (see § 310.32(h)).

(2) An expansion in the types or categories of information maintained.

(i) The addition of any new category of records not described under the ''Categories of Records in the System'' caption is considered an alteration.

(ii) Adding a new data element that is clearly within the scope of the categories of records described in the existing notice is an amendment. (see § 310.34(a)). An amended notice may not be required if the data element is clearly covered by the record category identified in the existing system notice.

(iii) All changes under this criterion require a change to the ''Categories of Records in the System'' caption of the notice. (see § 310.32(f)).

(3) An alteration of how the records are organized or the manner in which the records are indexed and retrieved.

(i) The change must alter the nature of use or scope of the records involved (for example, combining records systems in a reorganization).

(ii) Any change under this criteria requires a change in the ''Retrievability'' caption of the system notice. (see § 310.32(j)(2)).

(iii) If the records are no longer retrieved by name or personal identifier cancel the system notice. (see § 310.10(b)).

(4) A change in the purpose for which the information in the system is used.

(i) The new purpose must not be compatible with the existing purposes for which the system is maintained.

(ii) If the use is compatible and reasonably expected, there is no change in purpose and no alteration occurs.

(iii) Any change under this criterion requires a change in the ''Purpose(s)'' caption (see § 310.32(h)) and may require a change in the ''Authority for maintenance of the system'' caption (see § 310.32).

(5) Changes that alter the computer environment (such as changes to equipment configuration, software, or procedures) so as to create the potential for greater or easier access.

(i) Increasing the number of offices with direct access is an alteration.

(ii) Software applications, such as operating systems and system utilities, that provide for easier access are considered alterations.

(iii) The addition of an on-line capability to a previously batch-oriented system is an alteration.

(iv) The addition of peripheral devices such as tape devices, disk devices, card readers, printers, and similar devices to an existing IT system constitute an amendment if system security is preserved. (see § 310.34).

(v) Changes to existing equipment configuration with on-line capability need not be considered alterations to the system if:

(A) The change does not alter the present security posture; or

(B) The addition of terminals does not extend the capacity of the current operating system and existing security is preserved.

(vi) The connecting of two or more formerly independent automated systems or networks together creating a potential for greater access is an alteration.

(vii) Any change under this caption requires a change to the ''Storage'' caption element of the systems notice. (see § 310.32(j)(i)).

(c) *Reports of new and altered systems.* (1) Components shall submit a report for all new or altered systems to the DPO consistent with the requirements of this subpart and in the format prescribed at appendix F of this part.

(i) Components shall include the following when submitting an alteration for a system notice for publication in the FEDERAL REGISTER:

(A) The system identifier and name. (see § 310.32(b) and (c)).

(B) A description of the nature and specific changes proposed.

(ii) The full text of the system notice need not be submitted if the master registry contains a current system notice for the system. (see § 310.32(q)).

(2) The DPO coordinates all reports of new and altered systems with the Office of the Assistant Secretary of Defense (Legislative Affairs), Department of Defense.

(3) The DPO prepares and sends a transmittal letter that forwards the report, as well as the new or altered system notice, to OMB and Congress.

(4) The DPO shall publish in the FEDERAL REGISTER a system notice for new or altered systems.

(d) *Time restrictions on the operation of a new or altered system.* (1) The reports, and the new or altered system notice, must be provided OMB and Congress at least 40 days prior to the operation of the new or altered system. The 40 day review period begins on the date the transmittal letters are signed and dated.

(2) The system notice must be published in the FEDERAL REGISTER before a Component begins to operate the system (i.e., collect and use the information). If the new system has routine uses or the altered system adds a new routine use, no records may be disclosed pursuant to the routine use until the public has had 30 days to comment on the proposed use.

(3) The time periods run concurrently.

(e) *Exemptions for new systems.* See §310.30(e) for the procedures to follow in submitting exemption rules for a new system of records or for submitting an exemption rule for an existing system of records.

§310.34 Amendment and deletion of system notices.

(a) *Criteria for an amended system notice.* (1) Certain minor changes to published systems notices are considered amendments and not alterations. (see §310.33(b)).

(2) Amendments do not require a report of an altered system (see §310.33(c)), but must be published in the FEDERAL REGISTER.

(b) *System notices for amended systems.* Components shall include the following when submitting an amendment for a system notice for publication in the FEDERAL REGISTER:

(1) The system identifier and name. (see §310.32 (b) and (c)).

(2) A description of the nature and specific changes proposed.

(3) The full text of the system notice need not be submitted if the master registry contains a current system notice for the system. (see §310.32(q)).

(c) *Deletion of system notices.* (1) Whenever a system is discontinued, combined into another system, or determined no longer to be subject to this part, a deletion notice is required.

(2) The notice of deletion shall include:

(i) The system identification and name.

(ii) The reason for the deletion.

(3) When the system is eliminated through combination or merger, identify the successor system or systems in the deletion notice.

(d) *Submission of amendments and deletions for publication.* (1) Submit amendments and deletions to the DPO for transmittal to the FEDERAL REGISTER for publication.

(2) Multiple deletions and amendments may be combined into a single submission.

Subpart H—Training Requirements

§310.35 Statutory training requirements.

The Privacy Act (5 U.S.C. 552a) requires each Agency to establish rules of conduct for all persons involved in the design, development, operation, and maintenance of any system of record and to train these persons with respect to these rules.

§310.36 OMB training guidelines.

The OMB guidelines (OMB Privacy Guidelines, 40 FR 28948 (July 9, 1975) require all agencies additionally to:

(a) Instruct their personnel in their rules of conduct and other rules and procedures adopted in implementing the Act, to ensure that they are reminded of their specific responsibilities for safeguarding personally identifiable information, the rules for acquiring and using such information, and the penalties for non-compliance.

(b) Incorporate training on the special requirements of the Act into both formal and informal (on-the-job) training programs.

§ 310.37 DoD training programs.

(a) The training shall include information regarding information privacy laws, regulations, policies and procedures governing the Department's collection, maintenance, use, or dissemination of personal information. The objective is to establish a culture of sensitivity to, and knowledge about, privacy issues involving individuals throughout the Department.

(b) To meet these training requirements, Components may establish three general levels of training for those persons, to include contractor personnel, who are involved in any way with the design, development, operation, or maintenance of privacy protected systems of records. These are:

(1) *Orientation*. Training that provides basic understanding of this part as it applies to the individual's job performance. This training shall be provided to personnel, as appropriate, and should be a prerequisite to all other levels of training.

(2) *Specialized training*. Training that provides information as to the application of specific provisions of this part to specialized areas of job performance. Personnel of particular concern include, but are not limited to medical, personnel, and intelligence specialists, finance officers, DoD personnel who may be expected to deal with the news media or the public, special investigators, paperwork managers, and other specialists (reports, forms, records, and related functions), computer systems development personnel, computer systems operations personnel, statisticians dealing with personal data and program evaluations, contractors that will either operate systems of records on behalf of the Component or will have access to such systems incident to performing the contract, and anyone responsible for implementing or carrying out functions under this part.

(3) *Management*. Training designed to identify for responsible managers (such as, senior system managers, denial authorities, and decision-makers) considerations that they shall take into account when making management decisions regarding operational programs and activities having privacy implications.

(c) Include Privacy Act training in other courses of training when appropriate. Stress individual responsibilities and advise individuals of their rights and responsibilities under this part to ensure that it is understood that, where personally identifiable information is involved, individuals should handle and treat the information as if it was their information.

§ 310.38 Training methodology and procedures.

(a) Each DoD Component is responsible for the development of training procedures and methodology.

(b) The DPO shall assist the Components in developing these training programs and may develop privacy training programs for use by all DoD Components.

(c) Components shall conduct training as frequently as believed necessary so that personnel who are responsible for or are in receipt of information protected by 5 U.S.C. 552a are sensitive to the requirements of this part, especially the access, use, and dissemination restrictions. Components shall give consideration to whether annual training and/or annual certification should be mandated for all or specified personnel whose duties and responsibilities require daily interaction with personally identifiable information.

(d) Components shall conduct training that reaches the widest possible audience. Web-based training and video conferencing have been effective means to provide such training.

§ 310.39 Funding for training.

Each DoD Component shall fund its own privacy training program.

Subpart I—Reports

§ 310.40 Requirement for reports.

The DPO shall establish requirements for DoD Privacy Reports and the DoD Components may be required to provide data.

§ 310.41 Suspense for submission of reports.

The suspenses for submission of all reports shall be established by the DPO.

§ 310.42 Reports control symbol.

Any report established by this subpart in support of the Privacy Program shall be assigned Report Control Symbol DD–COMP(A)1379.

Subpart J—Inspections

§ 310.43 Privacy Act inspections.

During internal inspections, Component inspectors shall be alert for compliance with this part and for managerial, administrative, and operational problems associated with the implementation of the Defense Privacy Program. Programs shall be reviewed as frequently as considered necessary by Components or the Component Inspector General.

§ 310.44 Inspection reporting.

(a) Document the findings of the inspectors in official reports that are furnished the responsible Component officials. These reports, when appropriate, shall reflect overall assets of the Component Privacy Program inspected, or portion thereof, identify deficiencies, irregularities, and significant problems. Also document remedial actions taken to correct problems identified.

(b) Retain inspections reports and later follow-up reports in accordance with established records disposition standards. These reports shall be made available to the Privacy Program officials concerned upon request.

Subpart K—Privacy Act Violations

§ 310.45 Administrative remedies.

Any individual who believes he or she has a legitimate complaint or grievance against the Department of Defense or any DoD employee concerning any right granted by this part shall be permitted to seek relief through appropriate administrative channels.

§ 310.46 Civil actions.

An individual may file a civil suit against a DoD Component if the individual believes his or her rights under the Act have been violated. (See 5 U.S.C. 552a(g).)

§ 310.47 Civil remedies.

In addition to specific remedial actions, the Privacy Act provides for the payment of damages, court costs, and attorney fees in some cases.

§ 310.48 Criminal penalties.

(a) The Act also provides for criminal penalties. (See 5 U.S.C. 552a(i).) Any official or employee may be found guilty of a misdemeanor and fined not more than $5,000 if he or she willfully:

(1) Discloses information from a system of records, knowing dissemination is prohibited to anyone not entitled to receive the information (see subpart E of this part); or

(2) Maintains a system of records without publishing the required public notice in the FEDERAL REGISTER. (See subpart G of this part.)

(b) Any person who knowingly and willfully requests or obtains access to any record concerning another individual under false pretenses may be found guilty of misdemeanor and fined up to $5,000.

§ 310.49 Litigation status sheet.

Whenever a complaint citing the Privacy Act is filed in a U.S. District Court against the Department of Defense, a DoD Component, or any DoD employee, the responsible system manager shall notify the DPO. The litigation status sheet at appendix H to this part provides a standard format for this notification. The initial litigation status sheet forwarded shall, as a minimum, provide the information required by items 1 through 6 of the status sheet. A revised litigation status sheet shall be provided at each stage of the litigation. When a court renders a formal opinion or judgment, copies of the judgment and opinion shall be provided to the DPO with the litigation status sheet reporting that judgment or opinion.

§ 310.50 Lost, stolen, or compromised information.

(a) When a loss, theft, or compromise of information occurs (see § 310.14), the breach shall be reported to:

(1) The United States Computer Emergency Readiness Team (US CERT) within one hour of discovering that a

breach of personally identifiable information has occurred. Components shall establish procedures to ensure that US CERT reporting is accomplished in accordance with the guidance set forth at *http://www.us-cert.gov*.

(i) The underlying incident that led to the loss or suspected loss of PII (e.g., computer incident, theft, loss of material, etc.) shall continue to be reported in accordance with established procedures (e.g., to designated Computer Network Defense (CND) Service Providers (reference (z)), law enforcement authorities, the chain of command, etc.).

(ii) [Reserved]

(2) The Senior Component Official for Privacy within 24 hours of discovering that a breach of personally identifiable information has occurred. The Senior Component Official for Privacy, or their designee, shall notify the Defense Privacy Office of the breach within 48 hours upon being notified that a loss, theft, or compromise has occurred. The notification shall include the following information:

(i) Identify the Component/organization involved.

(ii) Specify the date of the breach and the number of individuals impacted, to include whether they are DoD civilian, military, or contractor personnel; DoD civilian or military retirees; family members; other Federal personnel or members of the public, etc.

(iii) Briefly describe the facts and circumstances surrounding the loss, theft, or compromise.

(iv) Briefly describe actions taken in response to the breach, to include whether the incident was investigated and by whom; the preliminary results of the inquiry if then known; actions taken to mitigate any harm that could result from the breach; whether the affected individuals are being notified, and if this will not be accomplished within 10 working days, that action will be initiated to notify the Deputy Secretary (see §310.14); what remedial actions have been, or will be, taken to prevent a similar such incident in the future, e.g., refresher training conducted, new or revised guidance issued; and any other information considered pertinent as to actions to be taken to ensure that information is properly safeguarded.

(2) The Component shall determine whether administrative or disciplinary action is warranted and appropriate for those individuals determined to be responsible for the loss, theft, or compromise.

Subpart L—Computer Matching Program Procedures

§310.51 General.

(a) A computer matching program covers two kinds of matching programs (see OMB Matching Guidelines, 54 FR 25818 (June 19, 1989)). If covered, the matches are subject to the requirements of this subpart. The covered programs are:

(1) Matches using records from Federal personnel or payroll systems of records, or

(2) Matches involving Federal benefits program if:

(i) To determine eligibility for a Federal benefit,

(ii) To determine compliance with benefit program requirements, or

(iii) To effect recovery of improper payments or delinquent debts under a Federal benefit program.

(b) The requirements of this part do not apply if matches are:

(1) Performed solely to produce aggregated statistical data without any personal identifiers. Personally identifying data can be used for purposes of conducting the match. However, the results of the match shall be stripped of any data that would identify an individual. Under no circumstances shall match results be used to take action against specific individuals.

(2) Performed to support research or statistical projects. Personally identifying data can be used for purposes of conducting the match and the match results may contain identifying data about individuals. However, the match results shall not be used to make a decision that affects the rights, benefits, or privileges of specific individuals.

(3) Performed by an agency, or a component thereof, whose principal function is the enforcement of criminal laws, subsequent to the initiation of a

specific criminal or civil law enforcement investigation of a named individual or individuals.

(i) The match must flow from an investigation already underway which focuses on a named person or persons. ''Fishing expeditions'' in which the subjects are generically identified, such as ''program beneficiaries'' are not covered.

(ii) The match must be for the purpose of gathering evidence against the named individual or individuals.

(4) Performed for tax information-related purposes.

(5) Performed for routine administrative purposes using records relating to Federal personnel.

(i) The records to be used in the match must predominantly relate to Federal personnel (i.e., the percentage of records in the system of records that are about Federal personnel must be greater than of any other category).

(ii) The purpose of the match must not be for purposes of taking any adverse financial, personnel, disciplinary, or other unfavorable action against an individual.

(6) Performed using only records from systems of records maintained by an agency.

(i) The purpose of the match must not be for purposes of taking any adverse financial, personnel, disciplinary, or other unfavorable action against an individual.

(ii) A match of DoD personnel using records in a system of records for purposes of identifying fraud, waste, and abuse is not covered.

(7) Performed to produce background checks for security clearances of Federal or contractor personnel or performed for foreign counter-intelligence purposes.

§ 310.52 Computer matching publication and review requirements.

(a) DoD Components shall identify the systems of records that will be used in the match to ensure the publication requirements of subpart G have been satisfied. If the match will require disclosure of records outside the Department of Defense, Components shall ensure a routine use has been established, and that the publication and review requirements have been met, before any disclosures are made (see subpart G of this part).

(b) If a computer matching program is contemplated, the DoD Component shall contact the DPO and provide information regarding the contemplated match. The DoD DPO shall ensure that any proposed computer matching program satisfies the requirements of the Privacy Act (5 U.S.C. 552a) and OMB Matching Guidelines (54 FR 25818 (June 19, 1989)).

(c) A computer matching agreement (CMA) shall be prepared by the Component, consistent with the requirements of § 310.53 of this subpart and submitted to the DPO. If the CMA satisfies the requirements of the Privacy Act (5 U.S.C. 552a) and OMB Matching Guidelines (54 FR 25818 (June 19, 1989)), as well as this subpart, it shall be forwarded to the Defense Data Integrity Board (DIB) for approval or disapproval.

(1) If the CMA is approved by the DIB, the DPO shall prepare and forward a report to both Houses of Congress and to OMB as required by, and consistent with, OMB Circular A–130, ''Management of Federal Information Resources,'' February 8, 1996, as amended. Congress and OMB shall have 40 days to review and comment on the proposed match. Any comments received must be resolved before matching can take place.

(2) If the CMA is approved by the DIB, the DPO shall prepare and forward a match notice as required by OMB Circular A–130, ''Management of Federal Information Resources,'' February 8, 1996, as amended, for publication in the FEDERAL REGISTER. The public shall be given 30 days to comment on the proposed match. Any comments received must be resolved before matching can take place.

§ 310.53 Computer matching agreements (CMAs).

(a) If a match is to be conducted internally within DoD, a memorandum of understanding (MOU) shall be prepared. It shall contain the same elements as a CMA, except as otherwise indicated in paragraph (b)(4)(ii) of this section.

(b) A CMA shall contain the following elements:

(1) *Purpose*. Why the match is being proposed and what will be achieved by conducting the match.

(2) *Legal authority*. What is the Federal or state statutory or regulatory basis for conducting the match. The Privacy Act does not constitute independent authority for matching. Other legal authority shall be identified.

(3) *Justification and expected results*. Explain why computer matching as opposed to some other administrative means is being proposed and what the expected results will be, including a specific estimate of any savings (see paragraph (b)(13) of this section).

(4) *Records description*. Identify:

(i) The system of records or non-Federal records. For DoD systems of records, provide the FEDERAL REGISTER citation for the system notice;

(ii) The specific routine use in the system notice if records are to be disclosed outside the Department of Defense (see §310.22(c)). If records are disclosed within the Department of Defense for an internal match, disclosures are permitted pursuant to paragraph (a) of §310.22.

(iii) The number of records involved;

(iv) The data elements to be included in the match;

(v) The projected start and completion dates of the match. CMAs remain in effect for 18 months but can be renewed for an additional 12 months provided:

(A) The match will be conducted without any change, and

(B) Each party to the match certifies in writing that the program has been conducted in compliance with the CMA or MOU.

(vi) How frequently will the records be matched.

(5) *Records accuracy assessment*. Provide an assessment by the source and recipient agencies as to the quality of the information that will be used for the match. The poorer the quality, the more likely that the program will not be cost-effective.

(6) *Notice procedures*. Identify what direct and indirect means will be used to inform individuals that matching will take place.

(i) *Direct notice*. Indicate whether the individual is advised that matching may be conducted when he or she applies for a Federal benefit program. Such an advisory should normally be part of the Privacy Act Statement that is contained in the application for benefits. Individual notice sometimes is provided by a separate notice that is furnished the individual upon receipt of the benefit.

(ii) *Indirect notice*. Indicate whether the individual is advised that matching may be conducted by constructive notice. Indirect or constructive notice is achieved by publication of a routine use in the FEDERAL REGISTER when the matching is between agencies or is achieved by publication of the match notice in the FEDERAL REGISTER.

(7) *Verification procedures*. Explain how information produced as a result of the match will be independently verified to ensure any adverse information obtained is that of the individual identified in the match.

(8) *Due process procedures*. Describe what procedures will be used to notify individuals of any adverse information uncovered as a result of the match and to give such individuals an opportunity to either explain the information or how to contest the information. No adverse action shall be taken against the individual until the due process procedures have been satisfied.

(i) Unless other statutory or regulatory authority provides for a longer period of time, the individual shall be given 30 calendar days from the date of the notice to respond to the notice.

(ii) If an individual contacts the agency within the notice period and indicates his or her acceptance of the validity of the adverse information, the agency may take final action. If the period expires without a response, the agency may take final action.

(iii) If the agency determines that there is a potentially significant effect on public health or safety, it may take appropriate action notwithstanding the due process provisions.

(9) *Security procedures*. Describe the administrative, technical, and physical safeguards that will be established to preserve and protect the privacy and confidentiality of the records involved in the match. The level of security must be commensurate with the level of the sensitivity of the records.

(10) *Records usage, duplication, and redisclosure restrictions.* Describe any restrictions imposed by the source agency or by statute or regulation on the collateral uses of the records. Recipient agencies may not use the records obtained for matching purposes for any other purpose absent a specific statutory requirement or where the disclosure is essential to the conduct of the matching program.

(11) *Disposition procedures.* Clearly state that the records used in the match will be retained only for the time required for conducting the match. Once the matching purpose has been achieved, the records will be destroyed unless the records must be retained as directed by other legal authority. Unless the source agency requests that the records be returned, identify the means by which destruction will occur, i.e., shredding, burning, electronic erasure, etc.

(12) *Comptroller General access.* Include a statement that the Comptroller General may have access to all records of the recipient agency to monitor or verify compliance with the terms of the CMA.

(13) *Cost-benefit analysis.* (i) A cost-benefit analysis shall be conducted for the proposed computer matching program unless:

(A) The Data Integrity Board waives the requirement, or

(B) The matching program is required by a specific statute.

(ii) The analysis must demonstrate that the program is likely to be cost-effective. This analysis is to ensure agencies are following sound management practices. The analysis provides an opportunity to examine the programs and to reject those that will only produce marginal results.

APPENDIX A TO PART 310—SAFEGUARDING PERSONALLY IDENTIFIABLE INFORMATION (PII)

(See §310.13 of Subpart B)

A. GENERAL

1. The IT environment subjects personal information to special hazards as to unauthorized compromise, alteration, dissemination, and use. Therefore, special considerations must be given to safeguarding personal information in IT systems consistent with the requirements of DoD Directive 8500.1 and DoD Instruction 8500.2.

2. Personally identifiable information must also be protected while it is being processed or accessed in computer environments outside the data processing installation (such as, remote job entry stations, terminal stations, minicomputers, microprocessors, and similar activities).

3. IT facilities authorized to process classified material have adequate procedures and security for the purposes of this Regulation. However, all unclassified information subject to this Regulation must be processed following the procedures used to process and access information designated ''For Official Use Only.'' (See DoD 5200.1–R.)

B. RISK MANAGEMENT AND SAFEGUARDING STANDARDS

1. Establish administrative, technical, and physical safeguards that are adequate to protect the information against unauthorized disclosure, access, or misuse. (See OMB Circular A–130 and DoD Instruction 8500.2.)

2. Tailor safeguards to the type of system, the nature of the information involved, and the specific threat to be countered.

C. MINIMUM ADMINISTRATIVE SAFEGUARDS

The minimum safeguarding standards as set forth in §310.13(b) apply to all personal data within any IT system. In addition:

1. Consider the following when establishing IT safeguards:

a. The sensitivity of the data being processed, stored and accessed.

b. The installation environment.

c. The risk of exposure.

d. The cost of the safeguard under consideration.

2. Label or designate media products containing personal information that do not contain classified material in such a manner as to alert those using or handling the information of the need for special protection. Designating products ''For Official Use Only'' in accordance with the requirements of DoD 5200.1–R satisfies this requirement.

3. Mark and protect all computer products containing classified data in accordance with the requirements of DoD 5200.1–R and DoD Directive 8500.1.

4. Mark and protect all computer products containing ''For Official Use Only'' material in accordance with the requirements of DoD 5200.1–R.

5. Ensure that safeguards for protected information stored at secondary sites are appropriate.

6. If there is a computer failure, restore all protected information being processed at the time of the failure using proper recovery procedures to ensure data integrity.

7. Train personnel involved in processing information subject to this Regulation in proper safeguarding procedures.

D. PHYSICAL SAFEGUARDS

1. For all unclassified facilities, areas, and devices that process information subject to this Regulation, establish physical safeguards that protect the information against reasonably identifiable threats that could result in unauthorized access or alteration.

2. Develop access procedures for unclassified computer rooms, tape libraries, micrographic facilities, decollating shops, product distribution areas, or other direct support areas that process or contain personal information subject to this Regulation that control adequately access to these areas.

3. Safeguard on-line devices directly coupled to IT systems that contain or process information from systems of records to prevent unauthorized disclosure, use, or alteration.

4. Dispose of paper records following appropriate record destruction procedures. (See §310.13(c) and DoD 5200.1–R.)

E. TECHNICAL SAFEGUARDS

1. Components are to ensure that all PII not explicitly cleared for public release is protected according to Confidentially Level Sensitive, as established in DoD Instruction 8500.2. In addition, all DoD information and data owners shall conduct risk assessments of compilations of PII and identify those needing more stringent protection for remote access or mobile computing.

2. Encrypt unclassified personal information in accordance with current Information Assurance (IA) policies and procedures, as issued.

3. Remove personal data stored on magnetic storage media by methods that preclude reconstruction of the data.

4. Ensure that personal information is not inadvertently disclosed as residue when transferring magnetic media between activities.

5. Only DoD authorized devices shall be used for remote access. Any remote access, whether for user or privileged functions, must conform to IA controls specified in DoD Instruction 8500.2.

6. Remote access for processing PII should comply with the latest IA policies and procedures.

7. Minimize access to data fields necessary to accomplish an employee's task-normally, access shall be granted only to those data elements (fields) required for the employee to perform his or her job rather than granting access to the entire database.

8. Do not totally rely on proprietary software products to protect personnel data during processing or storage.

F. SPECIAL PROCEDURES

1. Managers shall:

a. Prepare and submit for publication all system notices and amendments and alterations thereto. (See §310.30(f).)

b. Identify required controls and individuals authorized access to PII and maintain updates to the access authorizations.

c. When required, ensure Privacy Impact Assessments are prepared consistent with the requirements of the DoD Deputy Chief Information Officer Memorandum, ''DoD Privacy Impact Assessment Guidance,'' October 28, 2005.

d. Train all personnel whose official duties require access to the system of records in the proper safeguarding and use of the information and ensure that they receive Privacy Act training.

G. RECORD DISPOSAL

1. Dispose of records subject to this Regulation so as to prevent compromise. (See §310.13(c).) Magnetic tapes or other magnetic medium may be cleared by degaussing, overwriting, or erasing. (See DoD Memorandum, ''Disposition of Unclassified DoD Computer Hard Drives,'' June 4, 2001.)

2. Do not use respliced waste computer products containing personal data.

APPENDIX B TO PART 310—SAMPLE NOTIFICATION LETTER

(See §310.14 of subpart C)

Dear Mr. John Miller:

On January 1, 2006, a Department of Defense (DoD) laptop computer was stolen from the parked car of a DoD employee in Washington, DC after normal duty hours while the employee was running a personal errand. The laptop contained personally identifying information on 100 DoD employees who were participating in the xxx Program. The compromised information is the name, social security number, residential address, date of birth, office and home email address, office and home telephone numbers of the Program participants.

The theft was immediately reported to local and DoD law enforcement authorities who are now conducting a joint inquiry into the loss.

We believe that the laptop was the target of the theft as opposed to any information that the laptop might contain. Because the information in the laptop was password protected and encrypted, we also believe that the probability is low that the information will be acquired and used for an unlawful purpose. However, we cannot say with certainty that this might not occur. We therefore believe that you should consider taking such actions as are possible to protect against the potential that someone might use the information to steal your identity.

You should be guided by the actions recommended by the Federal Trade Commission at its Web site at *http://www.consumer.gov/idtheft/con_steps.htm*. The FTC urges that you immediately place an initial fraud alert on your credit file. The Fraud alert is for a period of 90 days, during which, creditors are required to contact you before a new credit card is issued or an existing card changed. The site also provides other valuable information that can be taken now or in the future if problems should develop.

The DoD takes this loss very seriously and is reviewing its current policies and practices with a view of determining what must be changed to preclude a similar occurrence in the future. At a minimum, we will be providing additional training to personnel to ensure that they understand that personally identifiable information must at all times be treated in a manner that preserves and protects the confidentiality of the data.

We deeply regret and apologize for any inconvenience and concern this theft may cause you.

Should you have any questions, please call _____.

Sincerely,

Signature Block
(Directorate level or higher)

APPENDIX C TO PART 310—DOD BLANKET ROUTINE USES

(See paragraph (c) of §310.22 of subpart E)

A. 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.

B. 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.

C. 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.

D. 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.

E. 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, may be disclosed to the Office of Management and Budget 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.

F. 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 Department of Defense military and civilian personnel.

G. 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., sections 5516, 5517, 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.

H. 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 reductions, and any other information necessary for the OPM to carry out its legally authorized government-wide personnel management functions and studies.

I. ROUTINE USE—DISCLOSURE TO THE DEPARTMENT OF JUSTICE FOR LITIGATION

A record from a system of records maintained by a 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.

J. ROUTINE USE—DISCLOSURE TO MILITARY BANKING FACILITIES

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.

K. ROUTINE USE—DISCLOSURE OF INFORMATION TO THE GENERAL SERVICES ADMINISTRATION

A record from a system of records maintained by a 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.

L. ROUTINE USE—DISCLOSURE OF INFORMATION TO THE NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

A record from a system of records maintained by a 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.

M. ROUTINE USE—DISCLOSURE TO THE MERIT SYSTEMS PROTECTION BOARD

A record from a system of records maintained by a 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.

N. ROUTINE USE—COUNTERINTELLIGENCE PURPOSES

A record from a system of records maintained by a Component may be disclosed as a routine use outside the Department of Defense (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 that protect the national security of the United States.

APPENDIX D TO PART 310—PROVISIONS OF THE PRIVACY ACT FROM WHICH A GENERAL OR SPECIFIC EXEMPTION MAY BE CLAIMED

(See paragraph (d) of §310.26)

Exemptions		Section of the Privacy Act
(j)(2)	(k) (1–7)	
No	No	(b)(1) Disclosures within the Department of Defense.
No	No	(2) Disclosures to the public.
No	No	(3) Disclosures for a ''Routine Use.''
No	No	(4) Disclosures to the Bureau of Census.
No	No	(5) Disclosures for statistical research and reporting.
No	No	(6) Disclosures to the NARA.
No	No	(7) Disclosures for law enforcement purposes.
No	No	(8) Disclosures under emergency circumstances.

Exemptions		Section of the Privacy Act
(j)(2)	(k) (1–7)	
No	No	(9) Disclosures to the Congress.
No	No	(10) Disclosures to the GAO.
No	No	(11) Disclosures pursuant to court orders.
No	No	(12) Disclosure to consumer reporting agencies.
No	No	(c)(1) Making disclosure accountings.
No	No	(2) Retaining disclosure accountings.
Yes	Yes	(c)(3) Making disclosure accounting available to the individual.
Yes	No	(c)(4) Informing prior recipients of corrections.
Yes	Yes	(d)(1) Individual access to records.
Yes	Yes	(2) Amending records.
Yes	Yes	(3) Review of the Component's refusal to amend a record.
Yes	Yes	(4) Disclosure of disputed information.
Yes	Yes	(5) Access to information compiled in anticipation of civil action.
Yes	Yes	(e)(1) Restrictions on collecting information.
Yes	No	(e)(2) Collecting directly from the individual.
Yes	No	(3) Informing individuals from whom information is requested.
No	No	(e)(4)(A) Describing the name and location of the system.
No	No	(B) Describing categories of individuals.
No	No	(C) Describing categories of records.
No	No	(D) Describing routine uses.
No	No	(E) Describing records management policies and practices.
No	No	(F) Identifying responsible officials.
Yes	Yes	(e)(4)(G) Procedures for determining if a system contains a record on an individual.
Yes	Yes	(H) Procedures for gaining access.
Yes	Yes	(I) Describing categories of information sources.
Yes	No	(e)(5) Standards of accuracy.
No	No	(e)(6) Validating records before disclosure.
No	No	(e)(7) Records of First Amendment activities.
No	No	(e)(8) Notification of disclosure under compulsory legal process.
No	No	(e)(9) Rules of conduct.
No	No	(e)(10) Administrative, technical, and physical safeguards.
No	No	(11) Notice for new and revised routine uses.
Yes	Yes	(f)(1) Rules for determining if an individual is subject of a record.
Yes	Yes	(f)(2) Rules for handling access requests.
Yes	Yes	(f)(3) Rules for granting access.
Yes	Yes	(f)(4) Rules for amending records.
Yes	Yes	(f)(5) Rules regarding fees.
Yes	No	(g)(1) Basis for civil action.
Yes	No	(g)(2) Basis for judicial review and remedies for refusal to amend.
Yes	No	(g)(3) Basis for judicial review and remedies for denial of access.
Yes	No	(g)(4) Basis for judicial review and remedies for other failure to comply.
Yes	No	(g)(5) Jurisdiction and time limits.
Yes	No	(h) Rights of legal guardians.
No	No	(i)(1) Criminal penalties for unauthorized disclosure.
No	No	(2) Criminal penalties for failure to publish.
No	No	(3) Criminal penalties for obtaining records under false pretenses.
Yes[1]	No	(j) Rulemaking requirement.
N/A	No	(j)(1) General exemption for the Central Intelligence Agency.
N/A	No	(j)(2) General exemption for criminal law enforcement records.
Yes	No	(k)(1) Exemption for classified material.
N/A	No	(k)(2) Exemption for law enforcement material.
Yes	N/A	(k)(3) Exemption for records pertaining to Presidential protection.
Yes	N/A	(k)(4) Exemption for statistical records.
Yes	N/A	(k)(5) Exemption for investigatory material compiled for determining suitability for employment or service.
Yes	N/A	(k)(6) Exemption for testing or examination material.
Yes	N/A	(k)(7) Exemption for promotion evaluation materials used by the Armed Forces.
Yes	No	(l)(1) Records stored in GSA records centers.
Yes	No	(l)(2) Records archived before September 27, 1975.
Yes	No	(l)(3) Records archived on or after September 27, 1975.
Yes	No	(m) Applicability to Government contractors.
Yes	No	(n) Mailing lists.
Yes[1]	No	(o) Reports on new systems.
Yes[1]	No	(p) Annual report.

[1] See paragraph (d) of §310.26.

APPENDIX E TO PART 310—SAMPLE OF NEW OR ALTERED SYSTEM OF RECORDS NOTICE IN FEDERAL REGISTER FORMAT

(See paragraph (f) of §310.30)

NEW SYSTEM OF RECORDS NOTICE

DEPARTMENT OF DEFENSE

OFFICE OF THE SECRETARY

PRIVACY ACT OF 1974; SYSTEM OF RECORDS

AGENCY: Office of the Secretary, DoD.
ACTION: Notice to add a system of records.
SUMMARY: The Office of the Secretary of Defense proposes to add a system of records to its inventory of record systems subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended.
DATES: The changes will be effective on (insert date thirty days after publication in the FEDERAL REGISTER) unless comments are received that would result in a contrary determination.
ADDRESSES: Send comments to OSD Privacy Act Coordinator, Records Management Section, Washington Headquarters Services, 1155 Defense Pentagon, Washington, DC 20301–1155.
FOR FURTHER INFORMATION CONTACT: Ms. Mary Smith at (703) 000–0000.
SUPPLEMENTARY INFORMATION: The Office of the Secretary of Defense notices for systems of records subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended, have been published in the FEDERAL REGISTER and are available from the address above.

The proposed systems reports, as required by 5 U.S.C. 552a(r) of the Privacy Act of 1974, as amended, were submitted on January 20, 2006, to the House Committee on Government Reform, the Senate Committee on Homeland Security and Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to paragraph 4c of Appendix I to OMB Circular No. A–130, ''Federal Agency Responsibilities for Maintaining Records About Individuals,'' dated February 8, 1996 (February 20, 1996, 61 FR 6427).

Dated: February 1, 2006.

John Miller,

OSD Federal Register Liaison Officer, Department of Defense.

NSLRB 01

System name: The National Security Labor Relations Board (NSLRB).

System location: National Security Labor Relations Board (NSLRB), 1401 Wilson Boulevard, Arlington, VA 22209–2325.

Categories of individuals covered by the system: Current and former civilian Federal Government employees who have filed unfair labor practice charges, negotiability disputes, exceptions to arbitration awards, and impasses with the National Security Labor Relations Board (NSLRB) pursuant to the National Security Personnel System (NSPS).

Categories of records in the system: Documents relating to the proceedings before the Board, including the name of the individual initiating NSLRB action, statements of witnesses, reports of interviews and hearings, examiner's findings and recommendations, a copy of the original decision, and related correspondence and exhibits.

Authority for maintenance of the system: The National Defense Authorization Act for FY 2004, Public Law 108–136, Section 1101; 5 U.S.C. 9902(m), Labor Management Relations in the Department of Defense; and 5 CFR 9901.907, National Security Labor Relations Board.

Purpose(s): To establish a system of records that will document adjudication of unfair labor practice charges, negotiability disputes, exceptions to arbitration awards, and impasses filed with the National Security Labor Relations Board.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

To the Federal Labor Relations Authority (FLRA) or the Equal Employment Opportunity Commission, when requested, for performance of functions authorized by law.

To disclose, in response to a request for discovery or for appearance of a witness, information that is relevant to the subject matter involved in a pending judicial or administrative proceeding.

To provide information to officials of labor organizations recognized under 5 U.S.C. 71 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting work conditions.

The DoD ''Blanket Routine Uses'' set forth at the beginning of OSD's compilation of systems of records notices apply to this system.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage: Records are maintained on electronic storage media and paper.

Retrievability: Records will be retrieved in the system by the following identifiers: assigned case number; individual's name; labor organizations filing the unfair labor practice charges; negotiability disputes; exceptions to arbitration awards; date, month, year or filing; complaint type; and the organizational component from which the complaint arises.

Safeguards: Records are maintained in a controlled facility. Physical entry is restricted by the use of locks, guards, and is accessible only to authorized personnel. Access to records is limited to person(s) responsible for servicing the record in performance of their official duties and who are properly screened and cleared for need-to-know. Access to computerized data is restricted by passwords, which are changed periodically.

Retention and disposal: Records are disposed of 5 years after final resolution of case.

System manager(s) and address: Executive Director, National Security Personnel System, Program Executive Office, 1401 Wilson Boulevard, Arlington, VA 22209–2325.

Notification procedure: Individuals seeking to determine whether this system of records contains information about themselves should address written inquiries to the Executive Director, National Security Personnel System, Program Executive Office, 1401 Wilson Boulevard, Arlington, VA 22209–2325.

Request should contain name; assigned case number; approximate case date (day, month, and year); case type; the names of the individuals and/or labor organizations filed the unfair labor practice charges; negotiability disputes; exceptions to arbitration awards; and impasses.

Record access procedures: Individuals seeking access to records about themselves contained in this system of records should address written inquiries to the Executive Director, National Security Personnel System, Program Executive Office, 1401 Wilson Boulevard, Arlington, VA 22209–2325.

Request should contain name; assigned case number; approximate case date (day, month, and year); case type; the names of the individuals and/or labor organizations filed the unfair labor practice charges; negotiability disputes; exceptions to arbitration awards; and impasses.

Contesting record procedures: The OSD's rules for accessing records, for contesting contents and appealing initial agency determinations are published in OSD Administrative Instruction No. 81; 32 CFR part 311; or may be obtained from the system manager.

Record source categories: Individual; other officials or employees; and departmental and other records containing information pertinent to the NSLRB action.

Exemptions claimed for the system: None.

ALTERED SYSTEM OF RECORD NOTICE

DEPARTMENT OF DEFENSE

Defense Logistics Agency

Privacy Act of 1974; Systems of Records

AGENCY: Defense Logistics Agency.

ACTION: Notice to alter a system of records.

SUMMARY: The Defense Logistics Agency proposes to alter a system of records notice in its inventory of record systems subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended. The alteration adds two routine uses, revises the purpose category, and makes other administrative changes to the system notice.

DATES: This action will be effective without further notice on (insert date thirty days after publication in the FEDERAL REGISTER) unless comments are received that would result in a contrary determination.

ADDRESSES: Send comments to the Privacy Act Officer, Headquarters, Defense Logistics Agency, ATTN: DSS–B, 8725 John J. Kingman Road, Suite 2533, Fort Belvoir, VA 22060–6221.

FOR FURTHER INFORMATION CONTACT: Ms. Mary Smith at (703) 000–0000.

SUPPLEMENTARY INFORMATION: The Defense Logistics Agency notices for systems of records subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended, have been published in the FEDERAL REGISTER and are available from the address above.

The proposed system report, as required by 5 U.S.C. 552a(r) of the Privacy Act of 1974, as amended, was submitted on January 29, 2004, to the House Committee on Government Reform, the Senate Committee on Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to paragraph 4c of Appendix I to OMB Circular No. A–130, 'Federal Agency Responsibilities for Maintaining Records About Individuals,' dated February 8, 1996 (February 20, 1996, 61 FR 6427).

Dated: February 2, 2004.

John Miller,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

S253.10 DLA–G

System name: Invention Disclosure (February 22, 1993, 58 FR 10854).

Changes:

* * * * *

System identifier: Replace 'S253.10 DLA–G' with 'S100.70'.

* * * * *

Categories of individuals covered by the system: Delete 'to the DLA General Counsel' at the end of the sentence and replace with 'to DLA.'

* * * * *

Categories of records in the system: Delete entry and replace with 'Inventor's name, Social Security Number, address, and telephone numbers; descriptions of inventions; designs or drawings, as appropriate; evaluations of

patentability; recommendations for employee awards; licensing documents; and similar records. Where patent protection is pursued by DLA, the file may also contain copies of applications, Letters Patent, and related materials.'

* * * * *

Authority for maintenance of the system: Delete entry and replace with '5 U.S.C. 301, Departmental Regulations; 5 U.S.C. 4502, General provisions; 10 U.S.C. 2320, Rights in technical data; 15 U.S.C. 3710b, Rewards for scientific, engineering, and technical personnel of federal agencies; 15 U.S.C. 3711d, Employee activities; 35 U.S.C. 181–185, Secrecy of Certain Inventions and Filing Applications in Foreign Countries; E.O. 9397 (SSN); and E.O. 10096 (Inventions Made by Government Employees) as amended by E.O. 10930.'

* * * * *

Purpose(s): Delete entry and replace with 'Data is maintained for making determinations regarding and recording DLA interest in the acquisition of patents; for documenting the patent process; and for documenting any rights of the inventor. The records may also be used in conjunction with the employee award program, where appropriate.'

* * * * *

Routine uses of records maintained in the system, including categories of users and the purpose of such uses: Add two new paragraphs: 'To the U.S. Patent and Trademark Office for use in processing applications and performing related functions and responsibilities under Title 35 of the U.S. Code.

To foreign government patent offices for the purpose of securing foreign patent rights.'

* * * * *

Safeguards: Delete entry and replace with 'Access is limited to those individuals who require the records for the performance of their official duties. Paper records are maintained in buildings with controlled or monitored access. During non-duty hours, records are secured in locked or guarded buildings, locked offices, or guarded cabinets. The electronic records systems employ user identification and password or smart card technology protocols.'

* * * * *

Retention and disposal: Delete entry and replace with 'Records maintained by Headquarters and field Offices of Counsel are destroyed 26 years after file is closed. Records maintained by field level Offices of Counsel where patent applications are not prepared are destroyed 7 years after closure.'

* * * * *

Record source categories: Delete entry and replace with 'Inventors, reviewers, evaluators, officials of U.S. and foreign patent offices, and other persons having a direct interest in the file.'

* * * * *

S100.70

System name: Invention Disclosure.

System location: Office of the General Counsel, HQ DLA–DG, 8725 John J. Kingman Road, Stop 2533, Fort Belvoir, VA 22060–6221, and the offices of counsel of the DLA field activities. Official mailing addresses are published as an appendix to DLA's compilation of systems of records notices.

Categories of individuals covered by the system: Employees and military personnel assigned to DLA who have submitted invention disclosures to DLA.

Categories of records in the system: Inventor's name, Social Security Number, address, and telephone numbers; descriptions of inventions; designs or drawings, as appropriate; evaluations of patentability; recommendations for employee awards; licensing documents; and similar records. Where patent protection is pursued by DLA, the file may also contain copies of applications, Letters Patent, and related materials.

Authority for maintenance of the system: 5 U.S.C. 301, Departmental Regulations; 5 U.S.C. 4502, General provisions; 10 U.S.C. 2320, Rights in technical data; 15 U.S.C. 3710b, Rewards for scientific, engineering, and technical personnel of federal agencies; 15 U.S.C. 3711d, Employee activities; 35 U.S.C. 181–185, Secrecy of Certain Inventions and Filing Applications in Foreign Countries; E.O. 9397 (SSN); and E.O. 10096 (Inventions Made by Government Employees) as amended by E.O. 10930.

Purpose(s): Data is maintained for making determinations regarding and recording DLA interest in the acquisition of patents, for documenting the patent process, and for documenting any rights of the inventor. The records may also be used in conjunction with the employee award program, where appropriate.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or

information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

To the U.S. Patent and Trademark Office for use in processing applications and performing related functions and responsibilities under Title 35 of the U. S. Code.

To foreign government patent offices for the purpose of securing foreign patent rights.

Information may be referred to other government agencies or to non-government agencies or to non-government personnel (including contractors or prospective contractors) having an identified interest in a particular invention and the Government's rights therein.

The DoD 'Blanket Routine Uses' set forth at the beginning of DLA's compilation of systems of records notices apply to this system.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage: Records are maintained in paper and computerized form.

Retrievability: Filed by names of inventors.

Safeguards: Access is limited to those individuals who require the records for the performance of their official duties. Paper records are maintained in buildings with controlled or monitored access. During nonduty hours, records are secured in locked or guarded buildings, locked offices, or guarded cabinets. The electronic records systems employ user identification and password or smart card technology protocols.

Retention and disposal: Records maintain by the HQ and field Offices of Counsel are destroyed 26 years after file is closed. Records maintained by field level Offices of Counsel where patent applications are not prepared are destroyed 7 years after closure.

System manager(s) and address: Office of the General Counsel, Headquarters, Defense Logistics Agency, ATTN: DG, 8725 John J. Kingman Road, Stop 2533, Fort Belvoir, VA 22060–6221.

Notification procedure: Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to the Privacy Officer, Headquarters, Defense Logistics Agency, ATTN: DSS–B, 8725 John J. Kingman Road, Stop 6220, Fort Belvoir, VA 22060–6221, or the Privacy Officers at DLA field activities. Official mailing addresses are published as an appendix to DLA's compilation of systems of records notices.

Record access procedures: Individuals seeking access to information about themselves contained in this system should address written inquiries to the Privacy Officer, Headquarters, Defense Logistics Agency, ATTN: DSS–B, 8725 John J. Kingman Road, Stop 6220, Fort Belvoir, VA 22060–6221, or the Privacy Officers at the DLA field activities. Official mailing addresses are published as an appendix to DLA's compilation of systems of records notices.

Individuals should provide information that contains full name, current address and telephone numbers of requester.

For personal visits, each individual shall provide acceptable identification, e.g., driver's license or identification card.

Contesting record procedures: The DLA rules for accessing records, contesting contents, and appealing initial agency determinations are contained in 32 CFR part 323, or may be obtained from the Privacy Act Officer, Headquarters, Defense Logistics Agency, ATTN: DSS–B, 8725 John J. Kingman Road, Stop 6220, Fort Belvoir, VA 22060–6221.

Record source categories: Inventors, reviewers, evaluators, officials of U.S. and foreign patent offices, and other persons having a direct interest in the file.

Exemptions claimed for the system: None.

APPENDIX F TO PART 310—FORMAT FOR NEW OR ALTERED SYSTEM REPORT

(See paragraph (c) of §310.33)

The report on a new or altered system shall consist of a transmittal letter, a narrative statement, and include supporting documentation.

A. TRANSMITTAL LETTER

The transmittal letter shall be prepared by the Defense Privacy Office and shall contain assurances that the new or altered system does not duplicate any existing Component systems, DoD-wide systems or government-wide systems. The narrative statement, and the system notice, shall be attached thereto.

B. NARRATIVE STATEMENT

The statement shall include information on the following:

1. System Identifier and name;
2. Responsible official;
3. Purpose of establishing the system [for a new system only] or Nature of the changes proposed for the system [for altered system only];
4. Authority for maintenance of the System;
5. Probable or potential effects on the privacy of individuals;
6. Is the system, in whole or part, being maintained by a contractor;
7. Steps taken to minimize risk of unauthorized access;
8. Routine use compatibility;
9. OMB information collection requirements; and
10. Supporting documentation.

ATTACHMENT 1—SAMPLE FORMAT FOR NARRATIVE STATEMENT

DEPARTMENT OF DEFENSE

[COMPONENT NAME]

NARRATIVE STATEMENT ON A [NEW/ALTERED] SYSTEM OF RECORDS

UNDER THE PRIVACY ACT OF 1974

1. *System Identifier and Name*. This caption sets forth the identification and name of the system (see subparagraphs (b)(c) of §310.32).

2. *Responsible Official*. The name, title, address, and telephone number of the official responsible for the report and to whom inquiries and comments about the report may be directed by Congress, the Office of Management and Budget, or the Defense Privacy Office.

3. *Purpose of establishing the system or nature of the changes proposed for the system:* Describe the purpose of the new system or how an existing system is being changed.

4. *Authority for maintenance of the system*. See paragraph (g) of §310.32.

5. *Probable or potential effects on the privacy of individuals*. What effect, if any, will the new or altered system impact the personal privacy of the affected individuals.

6. *Is the system, in whole or in part, being maintained by a contractor*. If yes, Components shall ensure that the contract has incorporated the Federal Acquisition privacy clause (see paragraph (a)(1) of §310.12).

7. *Steps taken to minimize risk of unauthorized access*. Describe actions taken to reduce the vulnerability of the system to potential threats. See Appendix A to this part.

8. *Routine use compatibility*. Provide assurances that any records contained in the system that are disclosed outside the DoD shall be for a use that is compatible with the purpose for which the record was collected. Advise whether or not the blanket routine uses apply to this system.

9. *OMB collection requirements*. If information is to be collected from members of the public, the requirements of reference ( ) apply and OMB must be advised.

10. *Supporting documentation*. The following are typical enclosures that may be required:

a. An advance copy of the system notice for a new or altered system that is proposed for publication.

b. An advance copy of a proposed exemption rule if the new or altered system is to be exempted in accordance with subpart F.

c. Any other supporting documentation that may be pertinent or helpful in understanding the need for the system or clarifying its intended use.

ATTACHMENT 2—SAMPLE NARRATIVE STATEMENT

DEPARTMENT OF DEFENSE

OFFICE OF THE SECRETARY

NARRATIVE STATEMENT ON A NEW SYSTEM OF RECORDS

UNDER THE PRIVACY ACT OF 1974

1. *System identifier and name:* NSLRB 01, entitled ''The National Security Labor Relations Board (NSLRB).''

2. *Responsible official:* Mr. John Miller, National Security Labor Relations Board (NSLRB), 0000 Smith Boulevard, Arlington, VA 22209, Telephone (703) 000–0000.

3. *Purpose of establishing the system:* The Office of the Secretary of Defense is proposing to establish a system of records that will document adjudication of unfair labor practice charges, negotiability disputes, exceptions to arbitration awards, and impasses filed with the National Security Labor Relations Board.

4. *Authority for the maintenance of the system:* The National Defense Authorization Act for FY 2004, Pub Law 108–136, Section 1101; 5 U.S.C. 9902(m), Labor Management Relations in the Department of Defense; and 5 CFR 9901.907, National Security Labor Relations Board.

5. *Probable or potential effects on the privacy of individuals:* None

6. *Is the system, in whole or in part, being maintained by a contractor?* No

7. *Steps taken to minimize risk of unauthorized access:* Records are maintained in a controlled facility. Physical entry is restricted by the use of locks, guards, and is accessible only to authorized personnel. Access to records is limited to person(s) responsible for servicing the record in performance of their official duties and who are properly screened and cleared for need-to-know. Access to computerized data is restricted by passwords, which are changed periodically.

8. *Routine use compatibility:* Any release of information contained in this system of records outside of the DoD will be compatible with purposes for which the information is collected and maintained. The DoD ''Blanket Routine Uses'' apply to this system of records.

9. *OMB information collection requirements:* None.

10. *Supporting documentation:* None.

APPENDIX G TO PART 310—SAMPLE AMENDMENTS OR DELETIONS TO SYSTEM NOTICES IN FEDERAL REGISTER FORMAT

(See §310.34)

Amendment of system notice

DEPARTMENT OF DEFENSE

Department of the Army

Privacy Act of 1974; System of Records

AGENCY: Department of the Army, DoD.
ACTION: Notice to Amend a System of Records.
SUMMARY: The Department of the Army is proposing to amend a system of records notice in its existing inventory of records systems subject to the Privacy Act of 1974, (5 U.S.C. 552a), as amended.
DATES: This proposed action will be effective without further notice on (insert date thirty days after publication in FEDERAL REGISTER) unless comments are received which result in a contrary determination.
ADDRESSES: Department of the Army, Freedom of Information/Privacy Division, U.S. Army Records Management and Declassification Agency, ATTN: AHRC–PDD–FPZ, 7701 Telegraph Road, Casey Building, Suite 144, Alexandria, VA 22325–3905.
FOR FURTHER INFORMATION CONTACT: Ms. Mary Smith at (703) 000–0000.
SUPPLEMENTARY INFORMATION: The Department of the Army systems of records notices subject to the Privacy Act of 1974, (5 U.S.C. 552a), as amended, have been published in the FEDERAL REGISTER and are available from the address above.

The specific changes to the records systems being amended are set forth below followed by the notices, as amended, published in their entirety. The proposed amendments are not within the purview of subsection (r) of the Privacy Act of 1974, (5 U.S.C. 552a), as amended, which requires the submission of a new or altered system report.

Dated: February 3, 2006.

John Miller,

OSD Federal Register Liaison Officer, Department of Defense.

A0055 USEUCOM

System name: Europe Command Travel Clearance Records (August 23, 2004, 69 FR 51817).

Changes:

* * * * *

System name: Delete system identifier and replace with: ''A0055 USEUCOM DoD''.

* * * * *

A0055 USEUCOM DoD

System name: Europe Command Travel Clearance Records.

System location: Headquarters, United States European Command, Computer Network Operations Center, Building 2324, P.O. Box 1000, APO AE 09131–1000.

Categories of individuals covered by the system: Military, DoD civilians, and non-DoD personnel traveling under DoD sponsorship (e.g., contractors, foreign nationals and dependents) and includes temporary travelers within the United States European Command's (USEUCOM) area of responsibility as defined by the DoD Foreign Clearance Guide Program.

Categories of records in the system: Travel requests, which contain the individual's name; rank/pay grade; Social Security Number; military branch or department; passport number; Visa Number; office address and telephone number, official and personal email address, detailed information on sites to be visited, visitation dates and purpose of visit.

Authority for the maintenance of the system: 10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 8013, Secretary of the Air Force; DoD 4500.54–G, Department of Defense Foreign Clearance Guide; Public Law 99–399, Omnibus Diplomatic Security and Antiterrorism Act of 1986; 22 U.S.C. 4801, 4802, and 4805, Foreign Relations and Intercourse; E.O. 12333, United States Intelligence Activities; Army Regulation 55–46, Travel Overseas; and E.O. 9397 (SSN).

Purpose(s): To provide the DoD with an automated system to clear and audit travel within the United States European Command's area of responsibility and to ensure compliance with the specific clearance requirements outline in the DoD Foreign Clearance Guide; to provide individual travelers with intelligence and travel warnings; and to provide the Defense Attaché and other DoD authorized officials with information necessary to verify official travel by DoD personnel.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

To the Department of State Regional Security Officer, U.S. Embassy officials, and foreign police for the purpose of coordinating security support for DoD travelers.

The DoD 'Blanket Routine Uses' set forth at the beginning of the Army's compilation of systems of records notices also apply to this system.

Policies and practices for storing, retiring, accessing, retaining, and disposing of records.

Storage: Electronic storage media.

Retrievability: Retrieved by individual's surname, Social Security Number and/or passport number.

Safeguards: Electronic records are located in the United States European Command's Theater Requirements Automated Clearance System (TRACS) computer database with built in safeguards. Computerized records are maintained in controlled areas accessible only to authorized personnel with an official need to know access. In addition, automated files are password protected and in compliance with the applicable laws and regulations. Another built in safeguard of the system is records are access to the data through secure network.

Retention and disposal: Records are destroyed 3 months after travel is completed.

System manager(s) and address: Special Assistant for Security Matters, Headquarters, United States European Command, Unit 30400, P.O. Box 1000, APO AE 09131–1000.

Notification procedures: Individuals seeking to determine whether information about themselves is contained in this system of records should address written inquiries to the Special Assistant for Security Matters, Headquarters, United States European Command, Unit 30400, P.O. Box 1000, APO AE 09131–1000.

Requests should contain individual's full name, Social Security Number, and/or passport number.

Record access procedures: Individuals seeking to access information about themselves that is contained in this system of records should address written inquiries to the Special Assistant for Security Matters, Headquarters, United States European Command, Unit 30400, P.O. Box 1000, APO AE 09131–1000.

Requests should contain individual's full name, Social Security Number, and/or passport number.

Contesting record procedures: The Army's rules for accessing records and for contesting contents and appealing initial agency determinations are contained in Army Regulation 340–21; 32 CFR part 505; or may be obtained from the system manager.

Record source categories: From individuals.

Exemptions claimed for the system: None.

DELETION OF SYSTEM NOTICE

DEPARTMENT OF DEFENSE

Office of the Secretary

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary, DoD.

ACTION: Notice to delete systems of records.

SUMMARY: The Office of the Secretary of Defense is deleting a system of records notice from its existing inventory of records systems subject to the Privacy Act of 1974, (5 U.S.C. 552a), as amended.

DATES: This proposed action will be effective without further notice on (insert date thirty days after publication in FEDERAL REGISTER) unless comments are received which result in a contrary determination.

ADDRESSES: OSD Privacy Act Coordinator, Records Management Section, Washington Headquarters Services, 1155 Defense Pentagon, Washington, DC 20301–1155.

FOR FURTHER INFORMATION CONTACT: Ms. Mary Smith at (703) 000–0000.

SUPPLEMENTARY INFORMATION: The Office of the Secretary of Defense systems of records notices subject to the Privacy Act of 1974, (5 U.S.C. 552a), as amended, have been published in the FEDERAL REGISTER and are available from the address above.

The specific changes to the records system being amended are set forth below followed by the notice, as amended, published in its entirety. The proposed amendments are not within the purview of subsection (r) of the Privacy Act of 1974, (5 U.S.C. 552a), as amended, which requires the submission of a new or altered system report.

Dated: April 2, 2006.

John Miller,

OSD Federal Register Liaison Officer, Department of Defense.

DODDS 27

System name: DoD Domestic and Elementary School Employee File (May 9, 2003, 68 FR 24935).

Reason: The records contained in this system of records are covered by OPM/GOVT–1 (General Personnel Records), a government-wide system notice.

APPENDIX H TO PART 310—LITIGATION STATUS SHEET

(See §310.49)

LITIGATION STATUS SHEET

1. Case Number[1]
2. Requester
3. Document Title or Description[2]
4. Litigation
a. Date Complaint Filed
b. Court
c. Case File Number[1]
5. Defendants (DoD Component and individual)
6. Remarks (brief explanation of what the case is about)
7. Court Action
a. Court's Finding

[1] Number used by the Component for reference purposes.

[2] Indicate the nature of the case, such as, ''Denial of access,'' ''Refusal to amend,'' ''Incorrect records,'' or other violations of the Act (specify).

b. Disciplinary Action (as appropriate)
8. Appeal (as appropriate)
a. Date Complaint Filed
b. Court
c. Case File Number
d. Court's Finding
e. Disciplinary Action (as appropriate)

PART 311—OFFICE OF THE SECRETARY OF DEFENSE AND JOINT STAFF PRIVACY PROGRAM

Sec.
311.1 Purpose.
311.2 Applicability.
311.3 Definitions.
311.4 Policy.
311.5 Responsibilities.
311.6 Procedures.
311.7 OSD/JS Privacy Office Processes.
311.8 Procedures for exemptions.

AUTHORITY: 5 U.S.C. 552a.

SOURCE: 74 FR 56114, Oct. 30, 2009, unless otherwise noted.

§ 311.1 Purpose.

This part revises 32 CFR part 311 to update Office of the Secretary of Defense (OSD) and Joint Staff (JS) policy, assigns responsibilities, and prescribes procedures for the effective administration of the Privacy Program in OSD and the JS. This part supplements and implements part 32 CFR part 310, the DoD Privacy Program.

§ 311.2 Applicability.

This part:

(a) Applies to OSD, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, and all other activities serviced by Washington Headquarters Services (WHS) that receive privacy program support from OSD/JS Privacy Office, Executive Services Directorate (ESD), WHS (hereafter referred to collectively as the ''WHS-Serviced Components).''

(b) Covers systems of records maintained by the WHS-Serviced Components and governs the maintenance, access, change, and release information contained in those systems of records, from which information about an individual is retrieved by a personal identifier.

§ 311.3 Definitions.

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

(b) *Computer matching program.* A program that matches the personal records in computerized databases of two or more Federal agencies.

(c) *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.

(d) *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. Members of the United States Armed Forces are ''individuals.'' Corporations, partnerships, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities are not ''individuals'' when acting in an entrepreneurial capacity with the Department of Defense but are ''individuals'' otherwise (*e.g.*, security clearances, entitlement to DoD privileges or benefits, *etc.*).

(e) *Individual access.* Access to information pertaining to the individual by the individual or his or her designated agent or legal guardian.

(f) *Maintain.* To maintain, collect, use, or disseminate records contained in a system of records.

(g) *Personal information.* Information about an individual that identifies, links, 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; other demographic, biometric, personnel, medical, and financial information, *etc.* Such information also is known as *personally identifiable information* (*i.e.*, information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records,

including any other personal information which is linked or linkable to a specified individual).

(h) *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 WHS-Serviced 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.

(i) *System manager.* A WHS-Serviced Component official who has overall responsibility for a system of records. The system manager may serve at any level in OSD. Systems managers are indicated in the published systems of records notices. If more than one official is indicated as a system manager, initial responsibility resides with the manager at the appropriate level (*i.e.,* for local records, at the local activity).

(j) *System of records.* A group of records under the control of a WHS-Serviced Component from which personal information about an individual is retrieved by the name of the individual or by some other identifying number, symbol, or other identifying particular assigned, that is unique to the individual.

§ 311.4 Policy.

It is DoD policy, in accordance with 32 CFR part 310, that:

(a) Personal information contained in any system of records maintained by any DoD organization shall be safeguarded. To the extent authorized by section 552a of title 5, United States Code, commonly known and hereafter referred to as the ''Privacy Act'' and Appendix I of Office of Management and Budget Circular No. A–130 (available at *http://www.whitehouse.gov/omb/assets/omb/circulars/a130/a130trans4.pdf*), an individual shall be permitted to know what existing records pertain to him or her consistent with 32 CFR part 310.

(b) Each office maintaining records and information about individuals shall ensure that this data is protected from unauthorized collection, use, dissemination and/or disclosure of personal information. These offices shall permit individuals to have access to and have a copy made of all or any portion of records about them, except as provided in 32 CFR 310.17 and 310.18. The individuals will also have an opportunity to request that such records be amended as provided by 32 CFR 310.19 . Individuals requesting access to their records shall receive concurrent consideration under section 552 of title 5, United States Code (commonly known and hereafter referred to as the ''Freedom of Information Act'').

(c) Necessary records of a personal nature that are individually identifiable will be maintained in a manner that complies with the law and DoD policy. Any information collected by WHS-Serviced Components must be as accurate, relevant, timely, and complete as is reasonable to ensure fairness to the individual. Adequate safeguards must be provided to prevent misuse or unauthorized release of such information, consistent with the Privacy Act.

§ 311.5 Responsibilities.

(a) The Director, WHS, under the authority, direction, and control of the Director, Administration and Management, shall:

(1) Direct and administer the OSD/JS Privacy Program for the WHS-Serviced Components.

(2) Ensure implementation of and compliance with standard and procedures established in 32 CFR part 310.

(3) Coordinate with the WHS General Counsel on all WHS-Serviced Components denials of appeals for amending records and review actions to confirm denial of access to records.

(4) Provide advice and assistance to the WHS-Serviced Components on matters pertaining to the Privacy Act.

(5) Direct the OSD/JS Privacy Office to implement all aspects of 32 CFR part 310 as directed in § 311.7 of this part.

(b) The Heads of the WHS-Serviced Components shall:

(1) Designate an individual in writing as the point of contact for Privacy Act matters and advise the Chief, OSD/JS Privacy Office, of names of officials so designated.

(2) Designate an official in writing to deny initial requests for access to an

individual's records or changes to records and advise the Chief, OSD/JS Privacy Office of names of officials so designated.

(3) Provide opportunities for appointed personnel to attend periodic Privacy Act training.

(4) Report any new record system, or changes to an existing system, to the Chief, OSD/JS Privacy Office at least 90 days before the intended use of the system.

(5) Formally review each system of records notice on a biennial basis and update as necessary.

(6) In accordance with 32 CFR 310.12, include appropriate Federal Acquisition Regulation clause (48 CFR 24.104) in all contracts that provide for contractor personnel to access WHS-Serviced Component records systems covered by the Privacy Act.

(7) Review all implementing guidance prepared by the WHS-Serviced Components as well as all forms or other methods used to collect information about individuals to ensure compliance with 32 CFR part 310.

(8) Establish administrative processes in WHS-Serviced Component organizations to comply with the procedures listed in this part and 32 CFR part 310.

(9) Coordinate with WHS General Counsel on all proposed denials of access to records.

(10) Provide justification to the OSD/JS Privacy Office when access to a record is denied in whole or in part.

(11) Provide the record to the OSD/JS Privacy Office when the initial denial of a request for access to such record has been appealed by the requester or at the time of initial denial if an appeal seems likely.

(12) Maintain an accurate administrative record documenting the actions resulting in a denial for access to a record or for the correction of a record. The administrative record should be maintained so it can be relied upon and submitted as a complete record of proceedings if litigation occurs in accordance with 32 CFR part 310.

(13) Ensure all personnel are aware of the requirement to take appropriate Privacy Act training as required by 32 CFR part 310 and the Privacy Act.

(14) Forward all requests for access to records received directly from an individual to the OSD/JS Freedom of Information Act Requester Service Center for processing under 32 CFR part 310 and 32 CFR part 286.

(15) Maintain a record of each disclosure of information (other than routine use) from a system of records as required by 32 CFR part 310.

§ 311.6 Procedures.

(a) *Publication of Notice in the* FEDERAL REGISTER. (1) A notice shall be published in the FEDERAL REGISTER of any record system meeting the definition of a system of records in 32 CFR 310.4.

(2) The Heads of the WHS-Serviced Component shall submit notices for new or revised systems of records to the Chief, OSD/JS Privacy Office, for review at least 90 days prior to desired implementation.

(3) The Chief, OSD/JS Privacy Office shall forward completed notices to the Defense Privacy Office (DPO) for review in accordance with 32 CFR 310.30. Publication in the FEDERAL REGISTER starts a 30-day comment window which provides the public with an opportunity to submit written data, views, or arguments to the DPO for consideration before a system of record is established or modified.

(b) *Access to Systems of Records Information.* (1) As provided in the Privacy Act, records shall be disclosed only to the individual they pertain to and under whose individual name or identifier they are filed, unless exempted by the provisions in 32 CFR 310.31. If an individual is accompanied by a third party, the individual shall be required to furnish a signed access authorization granting the third party access according to 32 CFR 310.17.

(2) Individuals seeking access to records that pertain to themselves, and that are filed by name or other personal identifier, may submit the request in person or by mail, in accordance with these procedures:

(i) Any individual making a request for access to records in person shall provide personal identification to the appropriate system owner, as identified in the system of records notice published in the FEDERAL REGISTER, to

verify the individual's identity according to 32 CFR 310.17.

(ii) Any individual making a request for access to records by mail shall address such request to the OSD/JS FOIA Requester Service Center, Office of Freedom of Information, 1155 Pentagon, Washington, DC 20301–1155. To verify his or her identity, the requester shall include either a signed notarized statement or an unsworn declaration in the format specified by 32 CFR part 286.

(iii) All requests for records shall describe the record sought and provide sufficient information to enable the material to be located (*e.g.*, identification of system of records, approximate date it was initiated, originating organization, and type of document).

(iv) All requesters shall comply with the procedures in 32 CFR part 310 for inspecting and/or obtaining copies of requested records.

(v) If the requester is not satisfied with the response, he or she may file a written appeal as provided in paragraph (f)(8) of this section. The requester must provide proof of identity by showing a driver's license or similar credentials.

(3) There is no requirement that an individual be given access to records that are not in a group of records that meet the definition of a system of records in the Privacy Act. (For an explanation of the relationship between the Privacy Act and the Freedom of Information Act, and for guidelines to ensure requesters are given the maximum amount of information authorized by both Acts, *see* 32 CFR part 310.17

(4) Granting access to a record containing personal information shall not be conditioned upon any requirement that the individual state a reason or otherwise justify the need to gain access.

(5) No verification of identity shall be required of an individual seeking access to records that are otherwise available to the public.

(6) Individuals shall not be denied access to a record in a system of records about themselves because those records are exempted from disclosure under 32 CFR part 286. Individuals may only be denied access to a record in a system of records about themselves when those records are exempted from the access provisions of 32 CFR 310.26.

(7) Individuals shall not be denied access to their records for refusing to disclose their Social Security Number (SSN), unless disclosure of the SSN is required by statute, by regulation adopted before January 1, 1975, or if the record's filing identifier and only means of retrieval is by SSN (Privacy Act, note).

(c) *Access to Records or Information Compiled for Law Enforcement Purposes.* (1) Requests are processed under 32 CFR part 310 and 32 CFR part 286 to give requesters a greater degree of access to records on themselves.

(2) Records (including those in the custody of law enforcement activities) that have been incorporated into a system of records exempted from the access conditions of 32 CFR part 310, will be processed in accordance with 32 CFR 286.12. Individuals shall not be denied access to records solely because they are in the exempt system. They will have the same access that they would receive under 32 CFR part 286. (*See also* 32 CFR 310.17.)

(3) Records systems exempted from access conditions will be processed under 32 CFR 310.26 or 32 CFR 286.12, depending upon which regulation gives the greater degree of access. (*See also* 32 CFR 310.17.)

(4) Records systems exempted from access under 32 CFR 310.27 that are temporarily in the hands of a non-law enforcement element for adjudicative or personnel actions, shall be referred to the originating agency. The requester will be informed in writing of this referral.

(d) *Access to Illegible, Incomplete, or Partially Exempt Records.* (1) An individual shall not be denied access to a record or a copy of a record solely because the physical condition or format of the record does not make it readily available (*e.g.*, deteriorated state or on magnetic tape). The document will be prepared as an extract, or it will be exactly recopied.

(2) If a portion of the record contains information that is exempt from access, an extract or summary containing all of the information in the record that is releasable shall be prepared.

(3) When the physical condition of the record makes it necessary to prepare an extract for release, the extract shall be prepared so that the requester will understand it.

(4) The requester shall be informed of all deletions or changes to records.

(e) *Access to Medical Records.* (1) Medical records shall be disclosed to the individual and may be transmitted to a medical doctor named by the individual concerned.

(2) The individual may be charged reproduction fees for copies or records as outlined in 32 CFR 310.20.

(f) *Amending and Disputing Personal Information in Systems of Records.* (1) The Head of a WHS-Serviced Component, or designated official, shall allow individuals to request amendment to their records to the extent that such records are not accurate, relevant, timely, or complete.

(2) Requests shall be submitted in person or by mail to the office designated in the system of records notice. They should contain, as a minimum, identifying information to locate the record, a description of the items to be amended, and the reason for the change. Requesters shall be required to provide verification of their identity as stated in paragraphs (b)(2)(i) and (b)(2)(ii) of this section to ensure that they are seeking to amend records about themselves and not, inadvertently or intentionally, the records of others.

(3) Requests shall not be rejected nor required to be resubmitted unless additional information is essential to process the request.

(4) The appropriate system manager shall mail a written acknowledgment to an individual's request to amend a record within 10 workdays after receipt. Such acknowledgment shall identify the request and may, if necessary, request any additional information needed to make a determination. No acknowledgment is necessary if the request can be reviewed and processed and if the individual can be notified of compliance or denial within the 10-day period. Whenever practical, the decision shall be made within 30 working days. For requests presented in person, written acknowledgment may be provided at the time the request is presented.

(5) The Head of a WHS-Serviced Component, or designated official, shall promptly take one of three actions on requests to amend the records:

(i) If the WHS-Serviced Component official agrees with any portion or all of an individual's request, he or she will proceed to amend the records in accordance with existing statutes, regulations, or administrative procedures and inform the requester of the action taken in accordance with 32 CFR 310.19. The WHS-Serviced Component official shall also notify all previous holders of the record that the amendment has been made and shall explain the substance of the correction.

(ii) If the WHS-Serviced Component official disagrees with all or any portion of a request, the individual shall be informed promptly of the refusal to amend a record, the reason for the refusal, and the procedure to submit an appeal as described in paragraph (f)(8) of this section.

(iii) If the request for an amendment pertains to a record controlled and maintained by another Federal agency, the request shall be referred to the appropriate agency and the requester advised of this.

(6) When personal information has been disputed by the requestor, the Head of a WHS-Serviced Component, or designated official, shall:

(i) Determine whether the requester has adequately supported his or her claim that the record is inaccurate, irrelevant, untimely, or incomplete.

(ii) Limit the review of a record to those items of information that clearly bear on any determination to amend the record, and shall ensure that all those elements are present before a determination is made.

(7) If the Head of a WHS-Serviced Component, or designated official, after an initial review of a request to amend a record, disagrees with all or any portion of the request to amend a record, he or she shall:

(i) Advise the individual of the denial and the reason for it.

(ii) Inform the individual that he or she may appeal the denial.

(iii) Describe the procedures for appealing the denial, including the name

and address of the official to whom the appeal should be directed. The procedures should be as brief and simple as possible.

(iv) Furnish a copy of the justification of any denial to amend a record to the OSD/JS Privacy Office.

(8) If an individual disagrees with the initial WHS-Serviced Component determination, he or she may file an appeal. If the record is created and maintained by a WHS-Serviced Component, the appeal should be sent to the Chief, OSD/JS Privacy Office, WHS, 1155 Defense Pentagon, Washington, DC 20301–1155.

(9) If, after review, the Chief, OSD/JS Privacy Office, determines the system of records should not be amended as requested, the Chief, OSD/JS Privacy Office, shall provide a copy of any statement of disagreement to the extent that disclosure accounting is maintained in accordance with 32 CFR 310.25 and shall advise the individual:

(i) Of the reason and authority for the denial.

(ii) Of his or her right to file a statement of the reason for disagreeing with the OSD/JS Privacy Office's decision.

(iii) Of the procedures for filing a statement of disagreement.

(iv) That the statement filed shall be made available to anyone the record is disclosed to, together with a brief statement by the WHS-Serviced Component summarizing its reasons for refusing to amend the records.

(10) If the Chief, OSD/JS Privacy Office, determines that the record should be amended in accordance with the individual's request, the WHS-Serviced Component shall amend the record, advise the individual, and inform previous recipients where a disclosure accounting has been maintained in accordance with 32 CFR 310.25.

(11) All appeals should be processed within 30 workdays after receipt by the proper office. If the Chief, OSD/JS Privacy Office, determines that a fair and equitable review cannot be made within that time, the individual shall be informed in writing of the reasons for the delay and of the approximate date the review is expected to be completed.

(g) *Disclosure of Disputed Information.* (1) If the OSD/JS Privacy Office determines the record should not be amended and the individual has filed a statement of disagreement under paragraph (f)(8) of this section, the WHS-Serviced Component shall annotate the disputed record so it is apparent to any person to whom the record is disclosed that a statement has been filed. Where feasible, the notation itself shall be integral to the record. Where disclosure accounting has been made, the WHS-Serviced Component shall advise previous recipients that the record has been disputed and shall provide a copy of the individual's statement of disagreement in accordance with 32 CFR 310.21.

(i) This statement shall be maintained to permit ready retrieval whenever the disputed portion of the record is disclosed.

(ii) When information that is the subject of a statement of disagreement is subsequently disclosed, the WHS-Serviced Component designated official shall note which information is disputed and provide a copy of the individual's statement.

(2) The WHS-Serviced Component shall include a brief summary of its reasons for not making a correction when disclosing disputed information. Such statement shall normally be limited to the reasons given to the individual for not amending the record.

(3) Copies of the WHS-Serviced Component summary will be treated as part of the individual's record; however, it will not be subject to the amendment procedure outlined in paragraph (f) of this section.

(h) *Penalties.* (1) *Civil Action.* An individual may file a civil suit against the WHS-Serviced Component or its employees if the individual feels certain provisions of the Privacy Act have been violated.

(2) *Criminal Action.* (i) Criminal penalties may be imposed against an officer or employee of a WHS-Serviced Component for these offenses listed in the Privacy Act:

(A) Willful unauthorized disclosure of protected information in the records;

(B) Failure to publish a notice of the existence of a record system in the FEDERAL REGISTER; and

(C) Requesting or gaining access to the individual's record under false pretenses.

(ii) An officer or employee of a WHS-Serviced Component may be fined up to $5,000 for a violation as outlined in paragraphs (h)(2)(i)(A) through (h)(2)(i)(C) of this section.

(i) *Litigation Status Sheet.* Whenever a complaint citing the Privacy Act is filed in a U.S. District Court against the Department of Defense, a WHS-Serviced Component, or any employee of a WHS-Serviced Component, the responsible system manager shall promptly notify the OSD/JS Privacy Office, which shall notify the DPO. The litigation status sheet in Appendix H of 32 CFR part 310 provides a standard format for this notification. (The initial litigation status sheet shall, as a minimum, provide the information required by items 1 through 6). A revised litigation status sheet shall be provided at each stage of the litigation. When a court renders a formal opinion or judgment, copies of the judgment or opinion shall be provided to the OSD/JS Privacy Office with the litigation status sheet reporting that judgment or opinion.

(j) *Computer Matching Programs.* 32 CFR 310.52 prescribes that all requests for participation in a matching program (either as a matching agency or a source agency) be submitted to the DPO for review and compliance. The WHS-Serviced Components shall submit a courtesy copy to the OSD/JS Privacy Office at the time of transmittal to the DPO.

§ 311.7 OSD/JS Privacy Office Processes.

The OSD/JS Privacy Office shall:

(a) Exercise oversight and administrative control of the OSD/JS Privacy Program for the WHS-Serviced Components.

(b) Provide guidance and training to the WHS-Serviced Components as required by 32 CFR 310.37.

(c) Collect and consolidate data from the WHS-Serviced Components and submit reports to the DPO, as required by 32 CFR 310.40 or otherwise requested by the DPO.

(d) Coordinate and consolidate information for reporting all record systems, as well as changes to approved systems, to the DPO for final processing to the Office of Management and Budget, the Congress, and the FEDERAL REGISTER, as required by 32 CFR part 310.

(e) In coordination with DPO, serve as the appellate authority for the WHS-Serviced Components when a requester appeals a denial for access as well as when a requester appeals a denial for amendment or initiates legal action to correct a record.

(f) Refer all matters about amendments of records and general and specific exemptions under 32 CFR 310.19, 310.28 and 310.29 to the proper WHS-Serviced Components.

§ 311.8 Procedures for exemptions.

(a) *General information.* The Secretary of Defense designates those Office of the Secretary of Defense (OSD) systems of records which will be exempt from certain provisions of the Privacy Act. There are two types of exemptions, general and specific. The general exemption authorizes the exemption of a system of records from all but a few requirements of the Act. The specific exemption authorizes exemption of a system of records or portion thereof, from only a few specific requirements. If an OSD Component originates a new system of records for which it proposes an exemption, or if it proposes an additional or new exemption for an existing system of records, it shall submit the recommended exemption with the records system notice as outlined in § 311.6. No exemption of a system of records shall be considered automatic for all records in the system. The systems manager shall review each requested record and apply the exemptions only when this will serve significant and legitimate Government purpose.

(b) *General exemptions.* The general exemption provided by 5 U.S.C. 552a(j)(2) may be invoked for protection of systems of records maintained by law enforcement activities. Certain functional records of such activities are not subject to access provisions of the Privacy Act of 1974. Records identifying criminal offenders and alleged offenders consisting of identifying data and notations of arrests, the type and disposition of criminal charges, sentencing, confinement, release, parole, and probation status of individuals are

protected from disclosure. Other records and reports compiled during criminal investigations, as well as any other records developed at any stage of the criminal law enforcement process from arrest to indictment through the final release from parole supervision are excluded from release.

(1) *System identifier and name:* DWHS P42.0, DPS Incident Reporting and Investigations Case Files.

(i) *Exemption.* Portions of this system that fall within 5 U.S.C. 552a(j)(2) are exempt from the following provisions of 5 U.S.C. 552a, Sections (c)(3) and (4); (d)(1) through (d)(5); (e)(1) through (e)(3); (e)(5); (f)(1) through (f)(5); (g)(1) through (g)(5); and (h) of the Act.

(ii) *Authority:* 5 U.S.C. 552a(j)(2).

(iii) *Reason:* The Defense Protective Service is the law enforcement body for the jurisdiction of the Pentagon and immediate environs. The nature of certain records created and maintained by the DPS requires exemption from access provisions of the Privacy Act of 1974. The general exemption, 5 U.S.C. 552a(j)(2), is invoked to protect ongoing investigations and to protect from access criminal investigation information contained in this record system, so as not to jeopardize any subsequent judicial or administrative process taken as a result of information contained in the file.

(2) *System identifier and name:* JS006.CND, Department of Defense Counternarcotics C4I System.

(i) *Exemption:* Portions of this system that fall within 5 U.S.C. 552a(j)(2) are exempt from the following provisions of 5 U.S.C. 552a, section (c) (3) and (4); (d)(1) through (d)(5); (e)(1) through (e)(3); (e)(4)(G) and (e)(4)(H); (e)(5); (f)(1) through (f)(5); (g)(1) through (g)(5) of the Act.

(ii) *Authority:* 5 U.S.C. 552a(j)(2).

(iii) *Reason:* From subsection (c)(3) because the release of accounting of disclosure would inform a subject that he or she is under investigation. This information would provide considerable advantage to the subject in providing him or her with knowledge concerning the nature of the investigation and the coordinated investigative efforts and techniques employed by the cooperating agencies. This would greatly impede USSOUTHCOM's criminal law enforcement.

(iv) For subsections (c)(4) and (d) because notification would alert a subject to the fact that an investigation of that individual is taking place, and might weaken the on-going investigation, reveal investigatory techniques, and place confidential informants in jeopardy.

(v) From subsections (e)(4)(G) and (H) because this system of records is exempt from the access provisions of subsection (d) pursuant to subsection (j).

(vi) From subsection (f) because the agency's rules are inapplicable to those portions of the system that are exempt and would place the burden on the agency of either confirming or denying the existence of a record pertaining to a requesting individual might in itself provide an answer to that individual relating to an on-going criminal investigation. The conduct of a successful investigation leading to the indictment of a criminal offender precludes the applicability of established agency rules relating to verification of record, disclosure of the record to that individual, and record amendment procedures for this record system.

(vii) For compatibility with the exemption claimed from subsection (f), the civil remedies provisions of subsection (g) must be suspended for this record system. Because of the nature of criminal investigations, standards of accuracy, relevance, timeliness and completeness cannot apply to this record system. Information gathered in criminal investigations is often fragmentary and leads relating to an individual in the context of one investigation may instead pertain to a second investigation.

(viii) From subsection (e)(1) because the nature of the criminal investigative function creates unique problems in prescribing a specific parameter in a particular case with respect to what information is relevant or necessary. Also, due to USSOUTHCOM's close liaison and working relationships with the other Federal, as well as state, local and foreign country law enforcement agencies, information may be received which may relate to a case under the investigative jurisdiction of another

agency. The maintenance of this information may be necessary to provide leads for appropriate law enforcement purposes and to establish patterns of activity which may relate to the jurisdiction of other cooperating agencies.

(ix) From subsection (e)(2) because collecting information to the greatest extent possible directly from the subject individual may or may not be practicable in a criminal investigation. The individual may choose not to provide information and the law enforcement process will rely upon significant information about the subject from witnesses and informants.

(x) From subsection (e)(3) because supplying an individual with a form containing a Privacy Act Statement would tend to inhibit cooperation by many individuals involved in a criminal investigation. The effect would be somewhat inimical to established investigative methods and techniques.

(xi) From subsection (e)(5) because the requirement that records be maintained with attention to accuracy, relevance, timeliness, and completeness would unfairly hamper the criminal investigative process. It is the nature of criminal law enforcement for investigations to uncover the commission of illegal acts at diverse stages. It is frequently impossible to determine initially what information is accurate, relevant, timely, and least of all complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significant as further investigation brings new details to light.

(xii) From subsection (e)(8) because the notice requirements of this provision could present a serious impediment to criminal law enforcement by revealing investigative techniques, procedures, and existence of confidential investigations.

(3)–(15) [Reserved]

(16) System identifier and name: DWHS E06, Enterprise Correspondence Control System (ECCS).

(i) *Exemption:* During the staffing and coordination of actions to, from, and within components in conduct of daily business, exempt materials from other systems of records may in turn become part of the case record in this document control system. To the extent that copies of exempt records from those ''other'' systems of records are entered into this system, the Office of the Secretary of Defense hereby claims the same exemptions for the records from those ''other'' systems that are entered into this system, as claimed for the original primary system of which they are a part.

(ii) *Authority:* 5 U.S.C. 552a (j)(2) and (k)(1) through (k)(7).

(iii) Records are only exempt from pertinent provisions of 5 U.S.C. 552a to the extent such provisions have been identified and an exemption claimed for the original record and the purposes underlying the exemption for the original record still pertain to the record which is now contained in this system of records. In general, the exemptions were claimed in order to protect properly classified information relating to national defense and foreign policy, to avoid interference during the conduct of criminal, civil, or administrative actions or investigations, to ensure protective services provided the President and others are not compromised, to protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations, to preserve the confidentiality and integrity of Federal testing materials, and to safeguard evaluation materials used for military promotions when furnished by a confidential source. The exemption rule for the original records will identify the specific reasons why the records are exempt from specific provisions of 5 U.S.C. 552a.

(c) *Specific exemptions.* All systems of records maintained by any OSD Component shall be exempt from the requirements of 5 U.S.C. 552a(d) pursuant to subsection (k)(1) of that section to the extent that the system contains any information properly classified under Executive Order 11265, 'National Security Information,' dated June 28, 552a(d) pursuant to subsection (k)(1) of that section to the extent that the system contains any information properly classified under E.O. 11265, 'National Security Information,' dated June 28, 1979, as amended, and required by the Executive Order to be kept classified 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. The Secretary of Defense has designated the following OSD system of records described below specifically exempted from the appropriate provisions of the Privacy Act pursuant to the designated authority contained therein:

(1) *System identifier and name:* DGC 16, Political Appointment Vetting Files.

(i) *Exemption.* Portions of this system of records that fall within the provisions of 5 U.S.C. 552a(k)(5) may be exempt from the following subsections (d)(1) through (d)(5).

(ii) *Authority.* 5 U.S.C. 552a(k)(5).

(iii) *Reasons.* From (d)(1) through (d)(5) because the agency is required to protect the confidentiality of sources who furnished information to the Government under an expressed promise of confidentiality or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. This confidentiality is needed to maintain the Government's continued access to information from persons who otherwise might refuse to give it. This exemption is limited to disclosures that would reveal the identity of a confidential source.

(2) *System identifier and name:* DWHS P28, The Office of the Secretary of Defense Clearance File.

(i) *Exemption.* This system of records is exempt from subsections (c)(3) and (d) of 5 U.S.C. 552a, which would require the disclosure of investigatory material compiled solely for the purpose of determining access to classified information but only to the extent that disclosure of such material would reveal the identity of a source who furnished information to the Government under an expressed promise that the identity of the source would be held in confidence or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. A determination will be made at the time of the request for a record concerning the specific information which would reveal the identity of the source.

(ii) *Authority.* 5 U.S.C. 552a(k)(5).

(iii) *Reasons.* This exemption is required to protect the confidentiality of the sources of information compiled for the purpose of determining access to classified information. This confidentiality helps maintain the Government's continued access to information from persons who would otherwise refuse to give it.

(3) *System identifier and name:* DGC 04, Industrial Personnel Security Clearance Case Files.

(i) *Exemption.* All portions of this system which fall under 5 U.S.C. 552a(k)(5) are exempt from the following provisions of title 5 U.S.C. 552a: (c)(3); (d).

(ii) *Authority.* 5 U.S.C. 552a(k)(5).

(iii) *Reasons.* This system of records is exempt from subsections (c)(3) and (d) of section 552a of 5 U.S.C. which would require the disclosure of investigatory material compiled solely for the purpose of determining access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an expressed promise that the identity of the source would be held in confidence, or prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. A determination will be made at the time of the request for a record concerning whether specific information would reveal the identity of a source. This exemption is required in order to protect the confidentiality of the sources of information compiled for the purpose of determining access to classified information. This confidentiality helps maintain the Government's continued access to information from persons who would otherwise refuse to give it.

(4) *System identifier and name:* DWHS P32, Standards of Conduct Inquiry File.

(i) *Exemption.* This system of records is exempted from subsections (c)(3) and (d) of 5 U.S.C. 552a, which would require the disclosure of: Investigatory material compiled for law enforcement purposes; or investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, or Federal contracts, but only to the extent that

the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. If any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or otherwise be eligible, as a result of the maintenance of investigatory material compiled for law enforcement purposes, the material shall be provided to that individual, except to the extent that its disclosure would reveal the identity of a source who furnished information to the Government under an express promise or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. At the time of the request for a record, a determination will be made concerning whether a right, privilege, or benefit is denied or specific information would reveal the identity of a source.

(ii) *Authority*. 5 U.S.C. 552a(k)(2) and (5).

(iii) *Reasons*. These exemptions are necessary to protect the confidentiality of the records compiled for the purpose of: enforcement of the conflict of interest statutes by the Department of Defense Standards of Conduct Counselor, General Counsel, or their designees; and determining suitability, eligibility or qualifications for Federal civilian employment, military service, or Federal contracts of those alleged to have violated or caused others to violate the Standards of Conduct regulations of the Department of Defense.

(5) *System identifier and name:* DUSDP 02, Special Personnel Security Cases.

(i) *Exemption:* All portions of this system which fall under 5 U.S.C. 552a(k)(5) are exempt from the following provisions of 5 U.S.C. 552a: (c)(3); (d).

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

(iii) *Reasons:* This system of records is exempt from subsections (c)(3) and (d) of 5 U.S.C. 552a which would require the disclosure of investigatory material compiled solely for the purpose of determining access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an expressed promise that the identity of the source would be held in confidence or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. A determination will be made at the time of the request for a record concerning whether specific information would reveal the identity of a source. This exemption is required in order to protect the confidentiality of the sources of information compiled for the purpose of determining access to classified information. This confidentiality helps maintain the Government's continued access to information from persons who would otherwise refuse to give it.

(6) *System identifier and name:* DODDS 02.0, Educator Application Files.

(i) *Exemption*. All portions of this system which fall within 5 U.S.C. 552a(k)(5) may be exempt from the following provisions of 5 U.S.C. 552a: (c)(3); (d).

(ii) *Authority*. 5 U.S.C. 552a(k)(5).

(iii) *Reasons*. It is imperative that the confidential nature of evaluation and investigatory material on teacher application files furnished the Department of Defense Dependent Schools (DoDDS) under promises of confidentiality be exempt from disclosure to the individual to insure the candid presentation of information necessary to make determinations involving applicants suitability for DoDDS teaching positions.

(7) System identifier and name: DGC 20, DoD Presidential Appointee Vetting File.

(i) *Exemption:* Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source. Portions of this system of records that may be exempt pursuant to 5 U.S.C. 552a(k)(5) are subsections (d)(1) through (d)(5).

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

(iii) *Reason:* From (d)(1) through (d)(5) because the agency is required to

protect the confidentiality of sources who furnished information to the Government under an expressed promise of confidentiality or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. This confidentiality is needed to maintain the Government's continued access to information from persons who otherwise might refuse to give it.

(8) *System identifier and name:* DWHS P29, Personnel Security Adjudications File.

(i) *Exemption:* Portions of this system of records that fall within the provisions of 5 U.S.C. 552a(k)(5) may be exempt from the following subsections (d)(1) through (d)(5).

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

(iii) *Reasons.* From (d)(1) through (d)(5) because the agency is required to protect the confidentiality of sources who furnished information to the Government under an expressed promise of confidentiality or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. This confidentiality is needed to maintain the Government's continued access to information from persons who otherwise might refuse to give it. This exemption is limited to disclosures that would reveal the identity of a confidential source. At the time of the request for a record, a determination will be made concerning whether a right, privilege, or benefit is denied or specific information would reveal the identity of a source.

(9) *System identifier and name:* JS004SECDIV, Joint Staff Security Clearance Files.

(i) *Exemption:* Portions of this system of records are exempt pursuant to the provisions of 5 U.S.C. 552a(k)(5) from subsections 5 U.S.C. 552a(d)(1) through (d)(5).

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

(iii) *Reasons:* From subsections (d)(1) through (d)(5) because the agency is required to protect the confidentiality of sources who furnished information to the Government under an expressed promise of confidentiality or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. This confidentiality is needed to maintain the Government's continued access to information from persons who otherwise might refuse to give it. This exemption is limited to disclosures that would reveal the identity of a confidential source. At the time of the request for a record, a determination will be made concerning whether a right, privilege, or benefit is denied or specific information would reveal the identity of a source.

(10) *System identifier and name:* DFMP 26, Vietnamese Commando Compensation Files.

(i) *Exemption:* Information classified under E.O. 12958, as implemented by DoD 5200.1–R, may be exempt pursuant to 5 U.S.C. 552a(k)(1).

(ii) *Authority:* 5 U.S.C. 552a(k)(1).

(iii) *Reasons:* From subsection 5 U.S.C. 552a(d) because granting access to information that is properly classified pursuant to E.O. 12958, as implemented by DoD 5200.1–R, may cause damage to the national security.

(11) *System identifier and name:* DUSP 11, POW/Missing Personnel Office Files.

(i) *Exemption:* Information classified under E.O. 12958, as implemented by DoD 5200.1–R, may be exempt pursuant to 5 U.S.C. 552a(k)(1).

(ii) *Authority:* 5 U.S.C. 552a(k)(1).

(iii) *Reasons:* From subsection 5 U.S.C. 552a(d) because granting access to information that is properly classified pursuant to E.O. 12958, as implemented by DoD 5200.1–R, may cause damage to the national security.

(12) *System identifier and name:* DFOISR 05, Freedom of Information Act Case Files.

(i) *Exemption:* During the processing of a Freedom of Information Act request, exempt materials from other systems of records may in turn become part of the case record in this system. To the extent that copies of exempt records from those 'other' systems of records are entered into this system, the Office of the Secretary of Defense claims the same exemptions for the records from those 'other' systems that are entered into this system, as claimed for the original primary system of which they are a part.

(ii) *Authority:* 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), (k)(3), (k)(4), (k)(5), (k)(6), and (k)(7).

(iii) *Reasons:* Records are only exempt from pertinent provisions of 5 U.S.C. 552a to the extent such provisions have been identified and an exemption claimed for the original record and the purposes underlying the exemption for the original record still pertain to the record which is now contained in this system of records. In general, the exemptions were claimed in order to protect properly classified information relating to national defense and foreign policy, to avoid interference during the conduct of criminal, civil, or administrative actions or investigations, to ensure protective services provided the President and others are not compromised, to protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations, to preserve the confidentiality and integrity of Federal testing materials, and to safeguard evaluation materials used for military promotions when furnished by a confidential source. The exemption rule for the original records will identify the specific reasons why the records are exempt from specific provisions of 5 U.S.C. 552a.

(13) *System identifier and name:* DFOISR 10, Privacy Act Case Files.

(i) *Exemption:* During the processing of a Privacy Act request (which may include access requests, amendment requests, and requests for review for initial denials of such requests), exempt materials from other systems of records may in turn become part of the case record in this system. To the extent that copies of exempt records from those 'other' systems of records are entered into this system, the Office of the Secretary of Defense hereby claims the same exemptions for the records from those 'other' systems that are entered into this system, as claimed for the original primary system of which they are a part.

(ii) *Authority:* 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), (k)(3), (k)(4), (k)(5), (k)(6), and (k)(7).

(iii) Records are only exempt from pertinent provisions of 5 U.S.C. 552a to the extent such provisions have been identified and an exemption claimed for the original record and the purposes underlying the exemption for the original record still pertain to the record which is now contained in this system of records. In general, the exemptions were claimed in order to protect properly classified information relating to national defense and foreign policy, to avoid interference during the conduct of criminal, civil, or administrative actions or investigations, to ensure protective services provided the President and others are not compromised, to protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations, to preserve the confidentiality and integrity of Federal testing materials, and to safeguard evaluation materials used for military promotions when furnished by a confidential source. The exemption rule for the original records will identify the specific reasons why the records are exempt from specific provisions of 5 U.S.C. 552a.

(14) System identifier and name: DHRA 02, PERSEREC Research Files.

(i) *Exemption:* (A) Investigative material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(B) Therefore, portions of this system may be exempt pursuant to 5 U.S.C. 552a(k)(5) from the following subsections of 5 U.S.C. 552a(c)(3), (d), and (e)(1).

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

(iii) Reasons: (A) From subsection (c)(3) and (d) when access to accounting disclosures and access to or amendment of records would cause the identity of a confidential source to be revealed. Disclosure of the source's identity not only will result in the Department breaching the promise of confidentiality made to the source, but it will impair the Department's future ability to compile investigatory material for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access to classified information. Unless sources can be

assured that a promise of confidentiality will be honored, they will be less likely to provide information considered essential to the Department in making the required determinations.

(B) From (e)(1) because in the collection of information for investigatory purposes, it is not always possible to determine the relevance and necessity of particular information in the early stages of the investigation. In some cases, it is only after the information is evaluated in light of other information that its relevance and necessity becomes clear. Such information permits more informed decisionmaking by the Department when making required suitability, eligibility, and qualification determinations.

(15) System identifier and name: DCIFA 01, CIFA Operational and Analytical Records.

(i) *Exemptions:* This system of records is a compilation of information from other Department of Defense and U.S. Government systems of records. To the extent that copies of exempt records from those 'other' systems of records are entered into this system, OSD hereby claims the same exemptions for the records from those 'other' systems that are entered into this system, as claimed for the original primary system of which they are a part.

(ii) *Authority:* 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), (k)(3), (k)(4), (k)(5), (k)(6), and (k)(7).

(iii) Records are only exempt from pertinent provisions of 5 U.S.C. 552a to the extent (1) such provisions have been identified and an exemption claimed for the original record and (2) the purposes underlying the exemption for the original record still pertain to the record which is now contained in this system of records. In general, the exemptions are claimed in order to protect properly classified information relating to national defense and foreign policy, to avoid interference during the conduct of criminal, civil, or administrative actions or investigations, to ensure protective services provided the President and others are not compromised, to protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations, and to preserve the confidentiality and integrity of Federal evaluation materials. The exemption rule for the original records will identify the specific reasons why the records are exempt from specific provisions of 5 U.S.C. 552a.

(16) *System identifier and name:* DMDC 15 DoD, Armed Services Military Accession Testing.

(i) *Exemption:* Testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service or military service may be exempt pursuant to 5 U.S.C. 552a(k)(6), if the disclosure would compromise the objectivity or fairness of the test or examination process. Therefore, portions of the system of records may be exempt pursuant to 5 U.S.C. 552a(d).

(ii) *Authority:* 5 U.S.C. 552a(k)(6).

(iii) *Reasons:* (A) An exemption is required for those portions of the Skill Qualification Test system pertaining to individual item responses and scoring keys to preclude compromise of the test and to ensure fairness and objectivity of the evaluation system.

(B) From subsection (d)(1) when access to those portions of the Skill Qualification Test records would reveal the individual item responses and scoring keys. Disclosure of the individual item responses and scoring keys will compromise the objectivity and fairness of the test as well as the validity of future tests resulting in the Department being unable to use the testing battery as an individual assessment tool.

(17) *System identifier and name:* DMDC 11, Investigative Records Repository.

(i) *Exemptions:* (A) Investigatory material compiled for law enforcement purposes may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source.

(B) Records maintained in connection with providing protective services to the President and other individuals

under 18 U.S.C. 3506, may be exempt pursuant to 5 U.S.C. 552a(k)(3).

(C) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(D) Any portion of this system that falls under the provisions of 5 U.S.C. 552a(k)(2), (k)(3), or (k)(5) may be exempt from the following subsections of 5 U.S.C. 552(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f).

(ii) *Authority:* 5 U.S.C. 552a(k)(2), (k)(3), or (k)(5).

(iii) *Reasons:* (A) From subsection (c)(3) because it will enable the Department 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).

(B) From subsections (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 source's identity would be held in confidence (or prior to the effective date of the Act, under an implied promise).

(C) From subsections (d) and (f) because requiring OSD to grant access to records and agency rules for access and amendment of records would unfairly impede the agency's investigation of allegations of unlawful activities. To require OSD to confirm or deny the existence of a record pertaining to a requesting individual may in itself provide an answer to that individual relating to an on-going investigation. The investigation of possible unlawful activities would be jeopardized by agency rules requiring verification of record, disclosure of the record to the subject, and record amendment procedures.

(18) *System identifier and name:* DMDC 12 DoD, Joint Personnel Adjudication System (JPAS).

(i) *Exemption:* Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

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

(iii) *Reasons:* (A) from subsections (c)(3) and (d) when access to accounting disclosure and access to or amendment of records would cause the identity of a confidential source to be revealed. Disclosure of the source's identity not only will result in the Department breaching the promise of confidentiality made to the source but it will impair the Department's future ability to compile investigatory material for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access to classified information. Unless sources can be assured that a promise of confidentiality will be honored, they will be less likely to provide information considered essential to the Department in making the required determinations.

(B) From subsection (e)(1) because in the collection of information for investigatory purposes, it is not always possible to determine the relevance and necessity of particular information in the early stages of the investigation. It is only after the information is evaluated in light of other information that its relevance and necessity becomes clear. Such information permits more informed decision-making by the Department when making required suitability, eligibility, and qualification determinations.

(19) System identifier and name: DA&M 01, Civil Liberties Program Case Management System.

(i) *Exemptions:* Records contained in this System of Records may be exempted from the requirements of subsections (c)(3); (d)(1), (2), (3), and (4); (e)(1) and (e)(4)(G), (H), and (I); and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1). Records may be exempted from these subsections or, additionally, from the requirements of subsections (c)(4); (e)(2), (3), and (8) of the Privacy Act of 1974 consistent with any exemptions claimed under 5 U.S.C. 552a (j)(2) or (k)(1), (k)(2), or (k)(5) by the originator of the record, provided the reason for the exemption remains valid and necessary. An exemption rule for this system has been promulgated in accordance with the requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c) and (e) and is published at 32 CFR part 311.

(ii) *Authority:* 5 U.S.C. 552a (j)(2), (k)(1), (k)(2), or (k)(5).

(iii) *Reasons:* (A) From subsections (c)(3) (accounting of disclosures) because an accounting of disclosures from records concerning the record subject would specifically reveal an intelligence or investigative interest on the part of the Department of Defense and could result in release of properly classified national security or foreign policy information.

(B) From subsections (d)(1), (2), (3) and (4) (record subject's right to access and amend records) because affording access and amendment rights could alert the record subject to the investigative interest of law enforcement agencies or compromise sensitive information classified in the interest of national security. In the absence of a national security basis for exemption, records in this system may be exempted from access and amendment to the extent necessary to honor promises of confidentiality to persons providing information concerning a candidate for position. Inability to maintain such confidentiality would restrict the free flow of information vital to a determination of a candidate's qualifications and suitability.

(C) From subsection (e)(1) (maintain only relevant and necessary records) because in the collection of information for investigatory purposes, it is not always possible to determine the relevance and necessity of particular information in the early stages of the investigation. It is only after the information is evaluated in light of other information that its relevance and necessity becomes clear. In the absence of a national security basis for exemption under subjection (k)(1), records in this system may be exempted from the relevance requirement pursuant to subjection (k)(5) because it is not possible to determine in advance what exact information may assist in determining the qualifications and suitability of a candidate for position. Seemingly irrelevant details, when combined with other data, can provide a useful composite for determining whether a candidate should be appointed.

(D) From subsections (e)(4)(G) and (H) (publication of procedures for notifying subject of the existence of records about them and how they may access records and contest contents) because the system is exempted from subsection (d) provisions regarding access and amendment, and from the subsection (f) requirement to promulgate agency rules. Nevertheless, the Office of the Secretary of Defense has published notice concerning notification, access, and contest procedures because it may, in certain circumstances, determine it appropriate to provide subjects access to all or a portion of the records about them in this system of records.

(E) From subsection (e)(4)(I) (identifying sources of records in the system of records) because identifying sources could result in disclosure of properly classified national defense or foreign policy information, intelligence sources and methods, and investigatory techniques and procedures. Notwithstanding its proposed exemption from this requirement the Office of the Secretary of Defense identifies record sources in broad categories sufficient to provide general notice of the origins of the information it maintains in this system of records.

(F) From subsection (f) (agency rules for notifying subjects to the existence of records about them, for accessing and amending records, and for assessing fees) because the system is exempt

from subsection (d) provisions regarding access and amendment of records by record subjects. Nevertheless, the Office of the Secretary of Defense has published agency rules concerning notification of a subject in response to his request if any system of records named by the subject contains a record pertaining to him and procedures by which the subject may access or amend the records. Notwithstanding exemption, the Office of the Secretary of Defense may determine it appropriate to satisfy a record subject's access request.

(20) *System identifier and name:* DMDC 13 DoD, Defense Clearance and Investigations Index.

(i) *Exemptions:* Investigatory material compiled for law enforcement purposes may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source. Any portion of this system that falls under the provisions of 5 U.S.C. 552a(k)(2) may be exempt from the following subjections of 5 U.S.C. 552a(c)(3); (d); (e)(1); (e)(4)(G), (H), and (I) and (f).

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

(iii) *Reasons:* (A) From subsection (c)(3) because it will enable OSD components 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).

(B) From subsections (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).

(C) From subsections (d) and (f) because requiring OSD to grant access to records and agency rules for access and amendment of records would unfairly impede the investigation of allegations of unlawful activities. To require OSD to confirm or deny the existence of a record pertaining to a requesting individual may in itself provide an answer to that individual relating to an ongoing investigation. The investigation of possible unlawful activities would be jeopardized by agency rules requiring verification of record, disclosure of the record to the subject, and record amendment procedures.

(21) System identifier and name: DWHS E05, Mandatory Declassification Review Files.

(i) *Exemption:* Information classified under E.O. 13526, as implemented by DoD 5200.1–R, may be exempt pursuant to 5 U.S.C. 552a(k)(1).

(ii) *Authority:* 5 U.S.C. 552a(k)(1).

(iii) *Reasons:* From subsection 5 U.S.C. 552a(d) because granting access to information that is properly classified pursuant to E.O. 13526, as implemented by DoD 5200.1–R, may cause damage to the national security.

(22) System identifier and name: DPFPA 05, Computer Aided Dispatch and Records Management System (CAD/RMS).

(i) *Exemptions:* Portions of this system that fall within 5 U.S.C. 552a(j)(2) and/or (k)(2) are exempt from the following provisions of 5 U.S.C. 552a, section (c)(3) and (4); (d); (e)(1) through (e)(3); (e)(4)(G) through (I); (e)(5); (e)(8); (f) and (g) of the Act, as applicable.

(ii) *Authority:* 5 U.S.C. 552a(j)(2) and (k)(2).

(iii) *Reasons:* (A) From subsections (c)(3) and (4) because making available to a record subject the accounting of disclosure from records concerning him or her would specifically reveal any investigative interest in the individual.

Revealing this information could reasonably be expected to compromise ongoing efforts to investigate a known or suspected offender by notifying the record subject that he or she is under investigation. This information could also permit the record subject to take measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid or impede the investigation.

(B) From subsection (d) because these provisions concern individual access to and amendment of certain records contained in this system, including law enforcement and investigatory records. Compliance with these provisions could alert the subject of an investigation of the fact and nature of the investigation, and/or the investigative interest of law enforcement agencies; compromise sensitive information related to national security; interfere with the overall law enforcement process by leading to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; could identify a confidential source or disclose information which would constitute an unwarranted invasion of another's personal privacy; reveal a sensitive investigative or constitute a potential danger to the health or safety of law enforcement personnel, confidential informants, and witnesses. Amendment of these records would interfere with ongoing law enforcement investigations and analysis activities and impose an excessive administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised.

(C) From subsections (e)(1) through (e)(3) because it is not always possible to determine what information is relevant and necessary at an early stage in a given investigation. Also, because DoD and other agencies may not always know what information about a known or suspected offender may be relevant to law enforcement for the purpose of conducting an operational response.

(D) From subsections (e)(4)(G) through (I) (Agency Requirements) because portions of this system are exempt from the access and amendment provisions of subsection (d).

(E) From subsection (e)(5) because the requirement that records be maintained with attention to accuracy, relevance, timeliness, and completeness would unfairly hamper the criminal investigative process. It is the nature of criminal law enforcement for investigations to uncover the commission of illegal acts at diverse stages. It is frequently impossible to determine initially what information is accurate, relevant, timely, and least of all complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significant as further investigation brings new details to light.

(F) From subsection (e)(8) because the requirement to serve notice on an individual when a record is disclosed under compulsory legal process could unfairly hamper law enforcement processes. It is the nature of law enforcement that there are instances where compliance with these provisions could alert the subject of an investigation of the fact and nature of the investigation, and/or the investigative interest of intelligence or law enforcement agencies; compromise sensitive information related to national security; interfere with the overall law enforcement process by leading to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; reveal a sensitive investigative or intelligence technique; or constitute a potential danger to the health or safety of law enforcement personnel, confidential informants, and witnesses.

(G) From subsection (f) because requiring the Agency to grant access to records and establishing agency rules for amendment of records would compromise the existence of any criminal, civil, or administrative enforcement activity. To require the confirmation or denial of the existence of a record pertaining to a requesting individual may in itself provide an answer to that individual relating to the existence of an on-going investigation. The investigation of possible unlawful activities would be jeopardized by agency rules requiring verification of the record, disclosure of the record to the subject, and record amendment procedures.

(H) From subsection (g) for compatibility with the exemption claimed from subsection (f), the civil remedies provisions of subsection (g) must be suspended for this record system. Because of the nature of criminal investigations, standards of accuracy, relevance, timeliness and completeness cannot apply to this record system. Information gathered in criminal investigations if often fragmentary and leads relating to an individual in the context of one investigation may instead pertain to a second investigation.

(23) System identifier and name: DMDC 17 DoD, Continuous Evaluation Records for Personnel Security.

(i) Exemption: In the course of carrying out records checks for continuous evaluation, exempt records from other systems of records may in turn become part of the case records maintained in this system. To the extent that copies of exempt records from those 'other' systems of records are maintained into this system, OSD claims the same exemptions for the records from those 'other' systems that are entered into this system, as claimed for the original primary system of which they are a part.

(ii) Authority: 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), (k)(3), (k)(5), (k)(6), and (k)(7).

(iii) Reasons: Records are only exempt from pertinent provisions of 5 U.S.C. 552a to the extent that such provisions have been identified and an exemption claimed for the original record and the purposes underlying the exemption for the original record still pertain to the record which is now maintained in this system of records. In general, the exemptions were claimed in order to protect properly classified information relating to national defense and foreign policy; to avoid interference during the conduct of criminal, civil, or administrative actions or investigations; to ensure protective services provided the President and others are not compromised; to protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations; to preserve the confidentiality and integrity of Federal testing materials; and to safeguard evaluation materials used for military promotions when furnished by a confidential source. The exemption rule for the original records will identify the specific reasons why the records are exempt from specific provisions of 5 U.S.C. 552a.

(24) System identifier and name: DPFPA 06, Internal Affairs Records System.

(i) Exemptions: Portions of this system that fall within 5 U.S.C. 552a(j)(2) and/or (k)(2) are exempt from the following provisions of 5 U.S.C. 552a, section (c)(3) and (4); (d); (e)(1) through (e)(3); (e)(4)(G) through (I); (e)(5); (f) and (g) of the Act, as applicable.

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

(iii) Reasons:

(A) From subsections (c)(3) and (4) because making available to a record subject the accounting of disclosure of investigations concerning him or her would specifically reveal an investigative interest in the individual. Revealing this information would reasonably be expected to compromise open or closed administrative or civil investigation efforts to a known or suspected offender by notifying the record subject that he or she is under investigation. This information could also permit the record subject to take measures to impede the investigation, *e.g.*, destroy evidence, intimidate potential witnesses, or flee the area to avoid or impede the investigation.

(B) From subsection (d) because these provisions concern individual access to and amendment of open or closed investigation records contained in this system, including law enforcement and investigatory records. Compliance with these provisions would provide the subject of an investigation of the fact and nature of the investigation, and/or the investigative interest of the Pentagon Force Protection Agency; compromise sensitive information related to national security; interfere with the overall law enforcement process by leading to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; could identify a confidential informant or disclose information which would constitute an unwarranted invasion of another's personal

privacy; reveal a sensitive investigative or constitute a potential danger to the health or safety of law enforcement personnel, confidential informants, and witnesses. Amendment of investigative records would interfere with open or closed administrative or civil law enforcement investigations and analysis activities and impose an excessive administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised.

(C) From subsections (e)(1) through (e)(3) because it is not always possible to determine what information is relevant and necessary in open or closed investigations.

(D) From subsections (e)(4)(G) through (I) (Agency Requirements) because portions of this system are exempt from the access and amendment provisions of subsection (d).

(E) From subsection (e)(5) because the requirement that investigative records be maintained with attention to accuracy, relevance, timeliness, and completeness would unfairly hamper the criminal, administrative, or civil investigative process. It is the nature of Internal Affairs investigations to uncover the commission of illegal acts and administrative violations. It is frequently impossible to determine initially what information is accurate, relevant, timely, and least of all complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significant as further investigation brings new details to light.

(F) From subsection (f) because requiring the Agency to grant access to records and establishing agency rules for amendment of records would compromise the existence of any criminal, civil, or administrative enforcement activity. To require the confirmation or denial of the existence of a record pertaining to a requesting individual may in itself provide an answer to that individual relating to the existence of an on-going investigation. The investigation of possible unlawful activities would be jeopardized by agency rules requiring verification of the record, disclosure of the record to the subject, and record amendment procedures.

(G) From subsection (g) for compatibility with the exemption claimed from subsection (f), the civil remedies provisions of subsection (g) must be suspended for this record system. Because of the nature of criminal, administrative and civil investigations, standards of accuracy, relevance, timeliness and completeness cannot apply to open or closed investigations in this record system. Information gathered in criminal investigations is often fragmentary and leads relating to an individual in the context of one investigation may instead pertain to a second investigation.

(25) *System identifier and name:* DPFPA 07, Counterintelligence Management Information System (CIMIS).

(i) *Exemptions:* Portions of this system that fall within 5 U.S.C. 552a (k)(2) are exempt from the following provisions of 5 U.S.C. 552a, section (c)(3); (d); (e)(1); (e)(4) (G) through (I); and (f) of the Act, as applicable.

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

(iii) *Reasons:*

(A) From subsections (c)(3) because making available to a record subject the accounting of disclosure from records concerning him or her would specifically reveal any investigative interest in the individual. Revealing this information could reasonably be expected to compromise ongoing efforts to investigate a known or suspected offender by notifying the record subject that he or she is under investigation. This information could also permit the record subject to take measures to impede the investigation, *e.g.*, destroy evidence, intimidate potential witnesses, or flee the area to avoid or impede the investigation.

(B) From subsection (d) because these provisions concern individual access to and amendment of certain records contained in this system, including counterintelligence, law enforcement, and investigatory records. Compliance with these provisions could alert the subject of an investigation of the fact and nature of the investigation, and/or the investigative interest of agencies; compromise sensitive information related to national security; interfere with the

overall counterintelligence and investigative process by leading to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; could identify a confidential source or disclose information which would constitute an unwarranted invasion of another's personal privacy; reveal a sensitive investigation or constitute a potential danger to the health or safety of law enforcement personnel, confidential informants, and witnesses. Amendment of these records would interfere with ongoing counterintelligence investigations and analysis activities and impose an excessive administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised.

(C) From subsection (e)(1) because it is not always possible to determine what information is relevant and necessary at an early stage in a given investigation. Also, because Pentagon Force Protection Agency and other agencies may not always know what information about a known or suspected offender may be relevant to for the purpose of conducting an operational response.

(D) From subsections (e)(4)(G) through (I) (Agency Requirements) because portions of this system are exempt from the access and amendment provisions of subsection (d).

(E) From subsection (f) because requiring the Agency to grant access to records and establishing agency rules for amendment of records would compromise the existence of any criminal, civil, or administrative enforcement activity. To require the confirmation or denial of the existence of a record pertaining to a requesting individual may in itself provide an answer to that individual relating to the existence of an on-going investigation.

Counterintelligence investigations would be jeopardized by agency rules requiring verification of the record, disclosure of the record to the subject, and record amendment procedures.

(26) *System identifier and name:* DMDC 16 DoD, Identity Management Engine for Security and Analysis (IMESA).

(i) *Exemption:* To the extent that copies of exempt records from JUSTICE/FBI–001, National Crime Information Center (NCIC) are entered into the Interoperability Layer Service records, the OSD hereby claims the same exemptions, (j)(2) and (k)(3), for the records as claimed in JUSTICE/FBI–001, National Crime Information Center (NCIC). Pursuant to 5 U.S.C. 552a portions of this system that fall within (j)(2) and (k)(3) are exempt from the following provisions of 5 U.S.C. 552a, section (c)(3) and (4); (d); (e)(1) through (3); (e)(4)(G) through (I); (e)(5) and (8); (f); and (g) (as applicable) of the Act.

(ii) *Authority:* 5 U.S.C. 552a(j)(2) and (k)(3).

(iii) *Reasons:* (A) from subsection (c)(3) because making available to a record subject the accounting of disclosure from records concerning him or her would specifically reveal any investigative interest in the individual. Revealing this information could reasonably be expected to compromise ongoing efforts to investigate a known or suspected terrorist by notifying the record subject that he or she is under investigation. This information could also permit the record subject to take measures to impede the investigation, *e.g.*, destroy evidence, intimidate potential witnesses, or flee the area to avoid or impede the investigation.

(B) From subsection (c)(4) because portions of this system are exempt from the access and amendment provisions of subsection (d).

(C) From subsection (d) because these provisions concern individual access to and amendment of certain records contained in this system, including law enforcement, counterterrorism, investigatory, and intelligence records. Compliance with these provisions could alert the subject of an investigation of the fact and nature of the investigation, and/or the investigative interest of intelligence or law enforcement agencies; compromise sensitive information related to national security; interfere with the overall law enforcement process by leading to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; could identify a confidential source or disclose information which would constitute an unwarranted invasion of another's personal privacy; reveal a sensitive investigative or intelligence technique; or

constitute a potential danger to the health or safety of law enforcement personnel, confidential informants, and witnesses. Amendment of these records would interfere with ongoing counterterrorism, law enforcement, or intelligence investigations and analysis activities and impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised.

(D) From subsection (e)(1) because it is not always possible to determine what information is relevant and necessary to complete an identity comparison between the individual seeking access and a known or suspected terrorist. Also, because DoD and other agencies may not always know what information about an encounter with a known or suspected terrorist will be relevant to law enforcement for the purpose of conducting an operational response.

(E) From subsection (e)(2) because application of this provision could present a serious impediment to counterterrorism, law enforcement, or intelligence efforts in that it would put the subject of an investigation, study, or analysis on notice of that fact, thereby permitting the subject to engage in conduct designed to frustrate or impede that activity. The nature of counterterrorism, law enforcement, or intelligence investigations is such that vital information about an individual frequently can be obtained only from other persons who are familiar with such individual and his/her activities. In such investigations, it is not feasible to rely upon information furnished by the individual concerning his own activities.

(F) From subsection (e)(3) to the extent that this subsection is interpreted to require DoD to provide notice to an individual if DoD or another agency receives or collects information about that individual during an investigation or from a third party. Should this subsection be so interpreted, exemption from this provision is necessary to avoid impeding counterterrorism, law enforcement, or intelligence efforts by putting the subject of an investigation, study, or analysis on notice of that fact, thereby permitting the subject to engage in conduct intended to frustrate or impede the activity.

(G) From subsection (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) because portions of this system are exempt from the access and amendment provisions of subsection (d).

(H) From subsection (e)(5) because the requirement that records be maintained with attention to accuracy, relevance, timeliness, and completeness could unfairly hamper law enforcement processes. It is the nature of law enforcement to uncover the commission of illegal acts at diverse stages. It is often impossible to determine initially what information is accurate, relevant, timely, and least of all complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further details are brought to light.

(I) From subsection (e)(8) because the requirement to serve notice on an individual when a record is disclosed under compulsory legal process could unfairly hamper law enforcement processes. It is the nature of law enforcement that there are instances where compliance with these provisions could alert the subject of an investigation of the fact and nature of the investigation, and/or the investigative interest of intelligence or law enforcement agencies; compromise sensitive information related to national security; interfere with the overall law enforcement process by leading to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; reveal a sensitive investigative or intelligence technique; or constitute a potential danger to the health or safety of law enforcement personnel, confidential informants, and witnesses.

(J) From subsection (f) because requiring the Agency to grant access to records and establishing agency rules for amendment of records would unfairly impede the agency's law enforcement mission. To require the confirmation or denial of the existence of a record pertaining to a requesting individual may in itself provide an answer to that individual relating to the existence of an on-going investigation. The investigation of possible unlawful activities would be jeopardized by agency

rules requiring verification of the record, disclosure of the record to the subject, and record amendment procedures.

(K) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act.

[74 FR 58205, Nov. 12, 2009, as amended at 74 FR 55778, Oct. 29, 2009; 76 FR 22612, Apr. 22, 2011; 76 FR 57645, Sept. 16, 2011; 76 FR 58104, Sept. 20, 2011; 77 FR 15586, Mar. 16, 2012; 77 FR 15588, 15589, Mar. 16, 2012; 77 FR 16676, Mar. 22, 2012; 79 FR 64507, 64508, Oct. 30, 2014; 79 FR 66291, Nov. 7, 2014; 80 FR 58608, 58610, Sept. 30, 2015; 80 FR 79259, Dec. 21, 2015]

EFFECTIVE DATE NOTE: At 81 FR 38951, June 15, 2016, §311.8 was amended by adding paragraph (c)(27), effective Sept. 13, 2016. For the convenience of the user, the added text is set forth as follows:

§311.8 Procedures for exemptions.

* * * * *

(c) * * *

(27) *System identifier and name:* DMDC 24 DoD, Defense Information System for Security (DISS).

(i) *Exemption:* Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

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

(iii) *Reasons:* (A) from subsections (c)(3) and (d) when access to accounting disclosure and access to or amendment of records would cause the identity of a confidential source to be revealed. Disclosure of the source's identity not only will result in the Department breaching the promise of confidentiality made to the source but it will impair the Department's future ability to compile investigatory material for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access to classified information. Unless sources can be assured that a promise of confidentiality will be honored, they will be less likely to provide information considered essential to the Department in making the required determinations.

(B) From subsection (e)(1) because in the collection of information for investigatory purposes, it is not always possible to determine the relevance and necessity of particular information in the early stages of the investigation. It is only after the information is evaluated in light of other information that its relevance and necessity becomes clear. Such information permits more informed decision-making by the Department when making required suitability, eligibility, and qualification determinations.

PART 312—OFFICE OF THE INSPECTOR GENERAL (OIG) PRIVACY PROGRAM

Sec.

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

SOURCE: 56 FR 51976, Oct. 17, 1991, unless otherwise noted.

§312.1 Purpose.

Pursuant to the requirements of the Privacy Act of 1974 (5 U.S.C. 552a) and 32 CFR part 310—DoD Privacy Program, the following rules of procedures are established with respect to access and amendment of records maintained by the Office of the Inspector General (OIG) on individual subjects of these records.

[68 FR 37969, June 26, 2003]

§312.2 Definitions.

(a) All terms used in this part which are defined in 5 U.S.C. 552a shall have the same meaning herein.

(b) As used in this part, the term ''agency'' means the Office of the Inspector General (OIG), Department of Defense.

§312.3 Procedure for requesting information.

Individuals should submit written inquiries regarding all OIG files to the Office of Communications and Congressional Liaison, ATTN: FOIA/PA Office, 400 Army Navy Drive, Arlington, VA

22202–4704. Individuals making a request in person must provide acceptable picture identification, such as a current driver's license.

[68 FR 37969, June 26, 2003]

§ 312.4 Requirements for identification.

Only upon proper identification will any individual be granted access to records which pertain to him/her. Identification is required both for accurate record identification and to avoid disclosing records to unauthorized individuals. Requesters must provide their full name and as much information as possible about the record being sought in order that a proper search for records can be accomplished. Inclusion of a telephone number for the requester is recommended to expedite certain matters. Requesters applying in person must provide an identification with photograph, such as a driver's license, military identification card, building pass, etc.

[59 FR 2746, Jan. 19, 1994]

§ 312.5 Access by subject individuals.

(a) No individual will be allowed access to any information compiled or maintained in reasonable anticipation of civil or criminal actions or proceedings or otherwise exempt under § 312.12. Requests for pending investigations will be denied and the requester instructed to forward another request giving adequate time for the investigation to be completed. Requesters shall be provided the telephone number so they can call and check on the status in order to know when to resubmit the request.

(b) Any individual may authorize the OIG to provide a copy of his/her records to a third part. This authorization must be in writing, must designate the recipient by name, must specify the records or portion to be provided to the recipient, and should accompany the initial request to the OIG.

[56 FR 51976, Oct. 17, 1991, as amended at 59 FR 2746, Jan. 19, 1994]

§ 312.6 Fees.

Requesters will be charged only for the reproduction of requested documents and special postal methods, such as express mail, if applicable. There will be no charge for the first copy of a record provided to any individual. Thereafter, fees will be computed as set forth in appropriate DoD Directives and Regulations.

§ 312.7 Request for correction or amendment.

(a) Requests to correct or amend a file shall be addressed to the system manager in which the file is located. The request must reasonably describe the record to be amended, the items to be changed as specifically as possible, the type of amendment (e.g., deletion, correction, amendment), and the reason for amendment. Reasons should address at least one of the following categories: Accuracy, relevance, timeliness, completeness, fairness. The request should also include appropriate evidence which provide a basis for evaluating the request. Normally all documents submitted, to include court orders, should be certified. Amendments under this part are limited to correcting factual matters and not matters of official judgment or opinions, such as performance ratings, promotion potential, and job performance appraisals.

(b) Requirements of identification as outlined in § 312.4 apply to requests to correct or amend a file.

(c) Incomplete requests shall not be honored, but the requester shall be contacted for the additional information needed to process the request.

(d) The amendment process is not intended to permit the alteration of evidence presented in the course of judicial or quasi-judicial proceedings. Any amendments or changes to these records normally are made through the specific procedures established for the amendment of such records.

(e) Nothing in the amendment process is intended or designed to permit a collateral attack upon what has already been the subject of a judicial or quasi-judicial determination. However, while the individual may not attack the accuracy of the judicial or quasi-judicial determination, he or she may challenge the accuracy of the recording of that action.

§ 312.8 OIG review of request for amendment.

(a) A written acknowledgement of the receipt of a request for amendment of a record will be provided to the requester within 20 working days, unless final action regarding approval or denial will constitute acknowledgement.

(b) Where there is a determination to grant all or a portion of a request to amend a record, the record shall be promptly amended and the requesting individual notified. Individuals, agencies or DoD components shown by disclosure accounting records to have received copies of the record, or to whom disclosure has been made, will be notified of the amendment by the responsible OIG official.

(c) Where there is a determination to deny all or a portion of a request to amend a record, OIG will promptly advise the requesting individual of the specifics of the refusal and the reasons; and inform the individual that he/she may request a review of the denial(s) from the OIG designated official.

[56 FR 51976, Oct. 17, 1991, as amended at 69 FR 7366, Feb. 17, 2004]

§ 312.9 Appeal of initial amendment decision.

(a) All appeals on an initial amendment decision should be addressed to the Office of Communications and Congressional Liaison, ATTN: FOIA/PA Office, 400 Army Navy Drive, Arlington, VA 22202–4704. The appeal should be concise and should specify the reasons the requester believes that the initial amendment action by the OIG was not satisfactory. Upon receipt of the appeal, the designated official will review the request and make a determination to approve or deny the appeal.

(b) If the OIG designated official decides to amend the record, the requester and all previous recipients of the disputed information will be notified of the amendment. If the appeal is denied, the designated official will notify the requester of the reason of the denial, of the requester's right to file a statement of dispute disagreeing with the denial, that such statement of dispute will be retained in the file, that the statement will be provided to all future users of the file, and that the requester may file suit in a federal district court to contest the OIG decision not to amend the record.

(c) The OIG designated official will respond to all appeals within 30 working days or will notify the requester of an estimated date of completion if the 30 day limit cannot be met.

[56 FR 51976, Oct. 17, 1991, as amended at 68 FR 37969, June 26, 2003]

§ 312.10 Disclosure of OIG records to other than subject.

No record containing personally identifiable information within a OIG system of records shall be disclosed by any means to any person or agency outside the Department of Defense, except with the written consent of the individual subject of the record or as provided for in the Act and DoD 5400.11–R (32 CFR part 286a).

§ 312.11 Penalties.

(a) An individual may bring a civil action against the OIG to correct or amend the record, or where there is a refusal to comply with an individual request or failure to maintain any records with accuracy, relevance, timeliness and completeness, so as to guarantee fairness, or failure to comply with any other provision of the Privacy Act. The court may order correction or amendment of records. The court may enjoin the OIG from withholding the records and order the production of the record.

(b) Where it is determined that the action was willful or intentional with respect to 5 U.S.C. 552a(g)(1) (C) or (D), the United States shall be liable for the actual damages sustained, but in no case less than the sum of $1,000 and the costs of the action with attorney fees.

(c) Criminal penalties may be imposed against an officer or employee of the OIG who discloses material, which he/she knows is prohibited from disclosure, or who willfully maintains a system of records without compliance with the notice requirements.

(d) Criminal penalties may be imposed against any person who knowingly and willfully requests or obtains any record concerning another individual from an agency under false pretenses.

(e) All of these offenses are misdemeanors with a fine not to exceed $5,000.

§ 312.12 Exemptions.

(a) *Exemption for classified records.* Any record in a system of records maintained by the Office of the Inspector General which falls within the provisions of 5 U.S.C. 552a(k)(1) may be exempt from the following subsections of 5 U.S.C. 552a: (c)(3), (d), (e)(1), (e)(4)(G) through (I) and (f) to the extent that a record system contains any record properly classified under Executive Order 12958 and that the record is required to be kept classified in the interest of national defense or foreign policy. This specific exemption rule, claimed by the Inspector General under authority of 5 U.S.C. 552a(k)(1), is applicable to all systems of records maintained, including those individually designated for an exemption herein as well as those not otherwise specifically designated for an exemption, which may contain isolated items of properly classified information

(b) The Inspector General of the Department of Defense claims an exemption for the following record systems under the provisions of 5 U.S.C. 552a(j) and (k)(1)–(k)(7) from certain indicated subsections of the Privacy Act of 1974. The exemptions may be invoked and exercised on a case-by-case basis by the Deputy Inspector General for Investigations or the Director, Communications and Congressional Liaison Office, and the Chief, Freedom of Information/Privacy Act Office, which serve as the Systems Program Managers. Exemptions will be exercised only when necessary for a specific, significant and legitimate reason connected with the purpose of the records system.

(c) No personal records releasable under the provisions of The Freedom of Information Act (5 U.S.C. 552) will be withheld from the subject individual based on these exemptions.

(d) *System Identifier:* CIG–04

(1) *System name:* Case Control System.

(2) *Exemption:* Any portion of this system which falls within the provisions of 5 U.S.C. 552a(j)(2) may be exempt from the following subsections of 5 U.S.C. 552a: (c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (H), (I), (e)(5), (e)(8), (f), and (g).

(3) *Authority:* 5 U.S.C. 552a(j)(2).

(4) *Reasons:* From subsection (c)(3) because the release of accounting of disclosure would inform a subject that he or she is under investigation. This information would provide considerable advantage to the subject in providing him or her with knowledge concerning the nature of the investigation and the coordinated investigative efforts and techniques employed by the cooperating agencies. This would greatly impede OIG's criminal law enforcement.

(5) From subsection (c)(4) and (d), because notification would alert a subject to the fact that an open investigation on that individual is taking place, and might weaken the on-going investigation, reveal investigatory techniques, and place confidential informants in jeopardy.

(6) From subsection (e)(1) because the nature of the criminal and/or civil investigative function creates unique problems in prescribing a specific parameter in a particular case with respect to what information is relevant or necessary. Also, due to OIG's close liaison and working relationships with other Federal, state, local and foreign country law enforcement agencies, information may be received which may relate to a case under the investigative jurisdiction of another agency. The maintenance of this information may be necessary to provide leads for appropriate law enforcement purposes and to establish patterns of activity which may relate to the jurisdiction of other cooperating agencies.

(7) From subsection (e)(2) because collecting information to the fullest extent possible directly from the subject individual may or may not be practical in a criminal and/or civil investigation.

(8) From subsection (e)(3) because supplying an individual with a form containing a Privacy Act Statement would tend to inhibit cooperation by many individuals involved in a criminal and/or civil investigation. The effect would be somewhat adverse to established investigative methods and techniques.

(9) From subsection (e)(4) (G) through (I) because this system of records is exempt from the access provisions of subsection (d).

(10) From subsection (e)(5) because the requirement that records be maintained with attention to accuracy, relevance, timeliness, and completeness would unfairly hamper the investigative process. It is the nature of law enforcement for investigations to uncover the commission of illegal acts at diverse stages. It is frequently impossible to determine initially what information is accurate, relevant, timely, and least of all complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light.

(11) From subsection (e)(8) because the notice requirements of this provision could present a serious impediment to law enforcement by revealing investigative techniques, procedures, and existence of confidential investigations.

(12) From subsection (f) because the agency's rules are inapplicable to those portions of the system that are exempt and would place the burden on the agency of either confirming or denying the existence of a record pertaining to a requesting individual might in itself provide an answer to that individual relating to an on-going investigation. The conduct of a successful investigation leading to the indictment of a criminal offender precludes the applicability of established agency rules relating to verification of record, disclosure of the record to that individual, and record amendment procedures for this record system.

(13) For comparability with the exemption claimed from subsection (f), the civil remedies provisions of subsection (g) must be suspended for this record system. Because of the nature of criminal investigations, standards of accuracy, relevance, timeliness, and completeness cannot apply to this record system. Information gathered in an investigation is often fragmentary and leads relating to an individual in the context of one investigation may instead pertain to a second investigation.

(e) *System Identification:* CIG–06.

(1) *System name:* Investigative Files.

(2) *Exemption:* Any portion of this system which falls within the provisions of 5 U.S.C. 552a(j)(2) may be exempt from the following subsections of 5 U.S.C. 552a (c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4) (G), (H), (I), (e)(5), (e)(8), (f), and (g).

(3) *Authority:* 5 U.S.C. 552a(j)(2).

(4) *Reasons:* From subsection (c)(3) because the release of accounting of disclosure would inform a subject that he or she is under investigation. This information would provide considerable advantage to the subject in providing him or her with knowledge concerning the nature of the investigation and the coordinated investigative efforts and techniques employed by the cooperating agencies. This would greatly impede OIG's criminal law enforcement.

(5) From subsection (c)(4) and (d), because notification would alert a subject to the fact that an open investigation on that individual is taking place, and might weaken the on-going investigation, reveal investigatory techniques, and place confidential informants in jeopardy.

(6) From subsection (e)(1) because the nature of the criminal and/or civil investigative function creates unique problems in prescribing a specific parameter in a particular case with respect to what information is relevant or necessary. Also, due to OIG's close liaison and working relationships with other Federal, state, local and foreign country law enforcement agencies, information may be received which may relate to a case under the investigative jurisdiction of another agency. The maintenance of this information may be necessary to provide leads for appropriate law enforcement purposes and to establish patterns of activity which may relate to the jurisdiction of other cooperating agencies.

(7) From subsection (e)(2) because collecting information to the fullest extent possible directly from the subject individual may or may not be practical in a criminal and/or civil investigation.

(8) From subsection (e)(3) because supplying an individual with a form containing a Privacy Act Statement would tend to inhibit cooperation by

many individuals involved in a criminal and/or civil investigation. The effect would be somewhat adverse to established investigative methods and techniques.

(9) From subsection (e)(4) (G) through (I) because this system of records is exempt from the access provisions of subsection (d).

(10) From subsection (e)(5) because the requirement that records be maintained with attention to accuracy, relevance, timeliness, and completeness would unfairly hamper the investigative process. It is the nature of law enforcement for investigations to uncover the commission of illegal acts at diverse stages. It is frequently impossible to determine initially what information is accurate, relevant, timely, and least of all complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light.

(11) From subsection (e)(8) because the notice requirements of this provision could present a serious impediment to law enforcement by revealing investigative techniques, procedures, and existence of confidential investigations.

(12) From subsection (f) because the agency's rules are inapplicable to those portions of the system that are exempt and would place the burden on the agency of either confirming or denying the existence of a record pertaining to a requesting individual might in itself provide an answer to that individual relating to an on-going investigation. The conduct of a successful investigation leading to the indictment of a criminal offender precludes the applicability of established agency rules relating to verification of record, disclosure of the record to that individual, and record amendment procedures for this record system.

(13) For comparability with the exemption claimed from subsection (f), the civil remedies provisions of subsection (g) must be suspended for this record system. Because of the nature of criminal investigations, standards of accuracy, relevance, timeliness, and completeness cannot apply to this record system. Information gathered in an investigation is often fragmentary and leads relating to an individual in the context of one investigation may instead pertain to a second investigation.

(f) *System identifier:* CIG–15.

(1) *System name:* Departmental Inquiries Case System.

(2) *Exemption:* Investigatory material compiled for law enforcement purposes may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source. Any portions of this system which fall under the provisions of 5 U.S.C. 552a(k)(2) may be exempt from the following subsection of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I).

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

(4) *Reasons:* From subsection (c)(3) because disclosures from this system could interfere with the just, thorough and timely resolution of the compliant or inquiry, and possibly enable individuals to conceal their wrongdoing or mislead the course of the investigation by concealing, destroying or fabricating evidence or documents.

(5) From subsection (d) because disclosures from this system could interfere with the just thorough and timely resolution of the compliant or inquiry, and possibly enable individuals to conceal their wrongdoing or mislead the course of the investigation by concealing, destroying or fabricating evidence or documents. Disclosures could also subject sources and witnesses to harassment or intimidation which jeopardize the safety and well-being of themselves and their families.

(6) From subsection (e)(1) because the nature of the investigation function creates unique problems in prescribing specific parameters in a particular case as to what information is relevant or necessary. Due to close liaison and working relationships with other Federal, state, local and foreign country law enforcement agencies, information may be received which may relate to a

case under the investigative jurisdiction of another government agency. It is necessary to maintain this information in order to provide leads for appropriate law enforcement purposes and to establish patterns of activity which may relate to the jurisdiction of other cooperating agencies.

(7) From subsection (e)(4) (G) through (H) because this system of records is exempt from the access provisions of subsection (d).

(8) From subsection (f) because the agency's rules are inapplicable to those portions of the system that are exempt and would place the burden on the agency of either confirming or denying the existence of a record pertaining to a requesting individual might in itself provide an answer to that individual relating to an on-going investigation. The conduct of a successful investigation leading to the indictment of a criminal offender precludes the applicability of established agency rules relating to verification of record, disclosure of the record to that individual, and record amendment procedures for this record system.

(g) *System Identifier:* CIG–16.

(1) *System name:* DOD Hotline Program Case Files.

(2) *Exemption:* Any portions of this system of records which fall under the provisions of 5 U.S.C. 552a(k)(2) and (k)(5) may be exempt from the following subsections of 5 U.S.C. 552a: (c)(3), (d), (e)(1), (e)(4)(G), (H), and (f).

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

(4) *Reasons:* From subsection (c)(3) because disclosures from this system could interfere with the just, thorough and timely resolution of the complaint or inquiry, and possibly enable individuals to conceal their wrongdoing or mislead the course of the investigation by concealing, destroying or fabricating evidence or documents.

(5) From subsection (d) because disclosures from this system could interfere with the just, thorough and timely resolution of the complaint or inquiry, and possibly enable individuals to conceal their wrongdoing or mislead the course of the investigation by concealing, destroying or fabricating evidence or documents. Disclosures could also subject sources and witnesses to harassment or intimidation which jeopardize the safety and well-being of themselves and their families.

(6) From subsection (e)(1) because the nature of the investigation functions creates unique problems in prescribing specific parameters in a particular case as to what information is relevant or necessary. Due to close liaison and working relationships with other Federal, state, local, and foreign country law enforcement agencies, information may be received which may relate to a case under the investigative jurisdiction of another government agency. It is necessary to maintain this information in order to provide leads for appropriate law enforcement purposes and to establish patterns of activity which may relate to the jurisdiction of other cooperating agencies.

(7) From subsection (e)(4)(G) through (H) because this system of records is exempt from the access provisions of subsection (d).

(8) From subsection (f) because the agency's rules are inapplicable to those portions of the system that are exempt and would place the burden on the agency of either confirming or denying the existence of a record pertaining to a requesting individual might in itself provide an answer to that individual relating to an on-going investigation. The conduct of a successful investigation leading to the indictment of a criminal offender precludes the applicability of established agency rules relating to verification of record, disclosure of the record to that individual, and record amendment procedures for this record system.

(h) *System Identifier:* CIG 01.

(1) *System name:* Privacy Act and Freedom of Information Act Case Files.

(2) *Exemption:* During the processing of a Freedom of Information Act (FOIA) and Privacy Act (PA) request, exempt materials from other systems of records may in turn become part of the case record in this system. To the extent that copies of exempt records from those ''other'' systems of records are entered into this system, the Inspector General, DoD, claims the same exemptions for the records from those ''other'' systems that are entered into this system, as claimed for the original

primary system of which they are a part.

(3) *Authority:* 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), (k)(3), (k)(4), (k)(5), (k)(6), and (k)(7).

(4) *Reasons:* Records are only exempt from pertinent provisions of 5 U.S.C. 552a to the extent such provisions have been identified and an exemption claimed for the original record and the purposes underlying the exemption for the original record still pertain to the record which is now contained in this system of records. In general, the exemptions were claimed in order to protect properly classified information relating to national defense and foreign policy, to avoid interference during the conduct of criminal, civil, or administrative actions or investigations, to ensure protective services provided the President and others are not compromised, to protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations, to preserve the confidentiality and integrity of Federal testing materials, and to safeguard evaluation materials used for military promotions when furnished by a confidential source. The exemption rule for the original records will identify the specific reasons why the records are exempt from specific provisions of 5 U.S.C. 552a.

(i) *System Identifier:* CIG–21

(1) *System name:* Congressional Correspondence Tracking System.

(2) *Exemption:* During the processing of a Congressional inquiry, exempt materials from other systems of records may in turn become part of the case record in this system. To the extent that copies of exempt records from those ''other'' systems of records are entered into this system, the Inspector General, DoD, claims the same exemptions for the records from those ''other'' systems that are entered into this system, as claimed for the original primary system of which they are a part.

(3) *Authority:* 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), (k)(3), (k)(4), (k)(5), (k)(6), and (k)(7)

(4) *Reasons:* Records are only exempt from pertinent provisions of 5 U.S.C. 552a to the extent such provisions have been identified and an exemption claimed for the original record and the purposes underlying the exemption for the original record still pertain to the record which is now contained in this system of records. In general, the exemptions were claimed in order to protect properly classified information relating to national defense and foreign policy, to avoid interference during the conduct of criminal, civil, or administrative actions or investigations, to ensure protective services provided the President and others are not compromised, to protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations, to preserve the confidentiality and integrity of Federal testing materials, and to safeguard evaluation materials used for military promotions when furnished by a confidential source. The exemption rule for the original records will identify the specific reasons why the records are exempt from specific provisions of 5 U.S.C. 552a.

(j) *System identifier:* CIG 23

(1) *System name:* Public Affairs Files.

(2) *Exemption:* During the course of processing a General Counsel action, exempt materials from other systems of records may in turn become part of the case records in this system. To the extent that copies of exempt records from those 'other' systems of records are entered into the Public Affairs Files, the Office of the Inspector General hereby claims the same exemptions for the records from those 'other' systems that are entered into this system, as claimed for the original primary systems of records which they are a part.

(3) *Authority:* 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), (k)(3), (k)(4), (k)(5), (k)(6), and (k)(7).

(4) *Reasons:* Records are only exempt from pertinent provisions of 5 U.S.C. 552a to the extent (1) such provisions have been identified and an exemption claimed for the original record and (2) the purposes underlying the exemption for the original record still pertain to the record which is now contained in this system of records. In general, the exemptions were claimed in order to protect properly classified information

relating to national defense and foreign policy, to avoid interference during the conduct of criminal, civil, or administrative actions or investigations, to ensure protective services provided the President and others are not compromised, to protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations, to preserve the confidentiality and integrity of Federal testing materials, and to safeguard evaluation materials used for military promotions when furnished by a confidential source. The exemption rule for the original records will identify the specific reasons why the records are exempt from specific provisions of 5 U.S.C. 552a.

(k) *System identifier:* CIG–29.

(1) *System Name:* Privacy and Civil Liberties Complaint Reporting System.

(2) *Exemptions:* Any portion of this record system which falls within the provisions of 5 U.S.C. 552a (j)(2), (k)(2)and (k)(5) may be exempt from the following subsections of 5 U.S.C. 552a: (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I).

(3) Authority: 5 U.S.C. 552a(j)(2), (k)(2), and (k)(5).

(4) Reasons: To ensure the integrity of the privacy and civil liberties process. The execution requires that information be provided in a free and open manner without fear of retribution or harassment in order to facilitate a just, thorough, and timely resolution of the complaint or inquiry. Disclosures from this system can enable individuals to conceal their wrongdoing or mislead the course of the investigation by concealing, destroying, or fabricating evidence or documents. In addition, disclosures can subject sources and witnesses to harassment or intimidation which may cause individuals not to seek redress for wrongs through privacy and civil liberties channels for fear of retribution or harassment. There is a clear need to protect national security information from inadvertent disclosure.

[56 FR 51976, Oct. 17, 1991, as amended at 57 FR 24547, June 10, 1992; 61 FR 2916, Jan. 30, 1996; 64 FR 72929, Dec. 29, 1999; 68 FR 37969, June 26, 2003; 69 FR 7366, Feb. 17, 2004; 71 FR 64632, Nov. 3, 2006; 79 FR 25506, May 5, 2014]

§ 312.13 Ownership of OIG investigative records.

(a) Criminal and or civil investigative reports shall not be retained by DoD recipient organizations. Such reports are the property of OIG and are on loan to the recipient organization for the purpose for which requested or provided. All copies of such reports shall be destroyed within 180 days after the completion of the final action by the requesting organization.

(b) Investigative reports which require longer periods of retention may be retained only with the specific written approval of OIG.

§ 312.14 Referral of records.

An OIG system of records may contain records other DoD Components or Federal agencies originated, and who may have claimed exemptions for them under the Privacy Act of 1974. When any action is initiated on a portion of any several records from another agency which may be exempt, consultation with the originating agency or component will be affected. Documents located within OIG system of records coming under the cognizance of another agency will be referred to that agency for review and direct response to the requester.

PART 313—THE CHAIRMAN OF THE JOINT CHIEFS OF STAFF AND THE JOINT STAFF PRIVACY PROGRAM

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

§ 313.1 Source of regulations.

The Office of the Joint Chiefs of Staff is governed by the Privacy Act implementation regulations of the Office of the Secretary of Defense, 32 CFR part 311.

[40 FR 55535, Nov. 28, 1975. Redesignated at 56 FR 55631, Oct. 29, 1991, as amended at 56 FR 57802, Nov. 14, 1991]

PART 314—DEFENSE ADVANCED RESEARCH PROJECTS AGENCY, PRIVACY ACT OF 1974

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

§ 314.1 Source of regulations.

The Defense Advanced Research Projects Agency is governed by the Privacy Act implementation regulations of the Office of the Secretary of Defense, 32 CFR part 311.

[40 FR 55535, Nov. 28, 1975. Redesignated at 56 FR 55631, Oct. 29, 1991, as amended at 56 FR 57802, Nov. 14, 1991]

PART 315—UNIFORMED SERVICES UNIVERSITY OF HEALTH SCIENCES, PRIVACY ACT OF 1974

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

§ 315.1 Source of regulations.

The Uniformed Services University of the Health Sciences, is governed by the Privacy Act implementation regulations of the Office of the Secretary of Defense, 32 CFR part 311.

[40 FR 55535, Nov. 28, 1975. Redesignated at 56 FR 55631, Oct. 29, 1991, as amended at 56 FR 57802, Nov. 14, 1991]

PART 316—DEFENSE INFORMATION SYSTEMS AGENCY PRIVACY PROGRAM

Sec.

AUTHORITY: Pub. L. 93–579, 88 Stat. 1986 (5 U.S.C. 552a).

SOURCE: 40 FR 55535, Nov. 28, 1975, unless otherwise noted. Redesignated at 57 FR 6074, Feb. 20, 1992.

§ 316.1 Purpose.

This part delineates responsibility and provides guidance for the implementation of Pub. L. 93–579 (Privacy Act of 1974).

§ 316.2 Applicability.

This part applies to Headquarters, Defense Information Systems Agency (DISA) and DISA field activities.

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

§ 316.3 Authority.

This part is published in accordance with the authority contained in 32 CFR part 310, August 1975.

[40 FR 55535, Nov. 28, 1975. Redesignated and amended at 57 FR 6074, Feb. 20, 1992]

§ 316.4 Definitions.

Add to the definitions contained in 32 CFR 310.6 the following:

System Manager: The DISA official who is responsible for policies and procedures governing a DISA System of Record. His title and duty address will be found in the paragraph entitled Sysmanager in DISA's Record System Notices which are published in the FEDERAL REGISTER in compliance with provisions of the Privacy Act of 1974.

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

§ 316.5 Policy.

It is the policy of DISA:

(a) To preserve the personal privacy of individuals, to permit an individual to know what records exist pertaining to him in the DISA, and to have access to and have a copy made of all or any portion of such records and to correct or amend such records.

(b) To collect, maintain, use, or disseminate any record of identifiable personal information 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.

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

§ 316.6 Procedures and responsibilities.

(a) The Counsel, DISA, is hereby designated the Privacy Act Officer for DISA and is responsible for insuring that an internal DISA Privacy Program is established and maintained. He will also insure that all echelons of DISA effectively comply with and implement 32 CFR part 310.

(b) The Civilian Assistant to the Chief of Staff will be responsible for the annual reporting requirements contained in 32 CFR 310.5.

(c) DISA System Managers and other appropriate DISA officials will:

(1) Insure compliance with the provisions of 32 CFR 310.9.

(2) Comply with the provisions of 32 CFR 286a.11. In this area the Assistant to the Director for Administration will provide assistance.

(3) Adhere to the following:

(i) Within DISA, the System Manager of any record system will assure that records pertaining to an individual will be disclosed, upon request, to the individual to whom the record pertains. The individual need not state a reason or otherwise justify the need to gain access. A person of the individual's choosing may accompany the individual when the record is disclosed. The System Manager may require the individual to furnish a written statement authorizing discussion of the individual's records in the presence of the accompanying person. If requested, the System Manager will have a copy made of all or any portion of the record pertaining to the individual in a form comprehensible to the requester.

(ii) The System Manager may release records to the individual's representative who has the written consent of the individual. The System Manager will require reasonable identification of individuals to assure that records are disclosed to the proper person. No verification of identity will be required of an individual seeking access to records which are otherwise available to any member of the public under the Freedom of Information Act. Identification requirements should be consistent with the nature of the records being disclosed. For disclosure of records to an individual in person, the System Manager will require that the individual show some form of identification. For records disclosed to an individual in person or by mail, the System Manager may require whatever identifying information is needed to locate the record; i.e., name, social security number, date of birth. If the sensitivity of the data warrants, the System Manager may require a signed notarized statement of identity. The System Manager may compare the signatures of the requester with those in the records to verify identity. An individual will not be denied access to his record for refusing to disclose his social security number unless disclosure is required by statute or by regulation adopted before 1 January 1975. An individual will not be denied access to records pertaining to him because the records are exempted from disclosure under the provisions of the Freedom of Information Act.

(iii) The System Manager will not deny access to a record or a copy thereof to an individual solely because its physical presence is not readily available (i.e. on magnetic tape) or because the context of the record may disclose sensitive information about another individual. To protect the personal privacy of other individuals who may be identified in a record, the System Manager shall prepare an extract to delete only that information which would not be releasable to the requesting individual under the Freedom of Information Act.

(iv) When the System Manager is of the opinion that the disclosure of medical information could have an adverse effect upon the individual to whom it pertains, the System Manager will promptly request the individual to submit the name and address of a doctor who will determine whether the medical record may be disclosed directly to the individual. The System Manager will then request the opinion of the doctor named by the individual on whether a medical record may be disclosed to the individual. The System Manager shall disclose the medical record to the individual to whom it pertains unless, in the judgment of the doctor, access to the record could have an adverse effect upon the individual's physical or mental health. In this

event the System Manager will transmit the record to the doctor and immediately inform the individual.

(v) The fees to be charged, if any, to an individual for making copies of his record, excluding the cost of any search for and review of the record, will be in accordance with the ''Schedule of Fees'' as set forth in 32 CFR 286.5 and 286.10.

(vi) The System Manager of the record will permit an individual to request amendment of a record pertaining to the individual. Requests to amend records shall be in person or in writing and shall be submitted to the System Manager who maintains the records. Such requests should contain as a minimum, identifying information needed to locate the record, a brief description of the item or items of information to be amended, and the reason for the requested change.

(vii) The System Manager will provide a written acknowledgment of the receipt of a request to amend a record to the individual who requested the amendment within 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date of receipt of such request. Such an acknowledgment may, if necessary, request any additional information needed to make a determination. No acknowledgment is required if the request can be reviewed and processed and the individual notified of compliance or denial within the 10 day period.

(viii) The System Manager will promptly take one of the following actions on requests to amend records:

(A) Refer the request to the agency or office that has control of and maintains the record in those instances where the record requested remains the property of the controlling office or agency.

(B) In accordance with existing statute, regulation, or administrative procedure, make any correction of any portion thereof which the individual believes is not accurate, relevant, timely or complete, or

(C) Inform the individual of the System Manager's refusal to amend the record in accordance with the individual's request, the reason for the refusal, and the individual's right to request a review of the refusal by the Director, DISA, through the DISA Privacy Act Board.

(ix) The DISA Privacy Act Board will be comprised of the DISA Counsel, as Chairman; the Assistant to the Director for Administration, and the Assistant to the Director for Personnel; or in their absence, their authorized representatives. The individual who disagrees with the refusal of the System Manager to amend his record may request a review of this refusal by the DISA Privacy Act Board. The request for the review may be made orally or in writing and shall be made to the System Manager. The System Manager will promptly forward the request for review to the Chairman of the Board to make a proper review. The Board will promptly review the matter. If, after review, the Board is unanimous in its decision that the record be amended in accordance with the request of the individual then the Chairman of the Board shall so notify the System Manager. The System Manager will immediately make the necessary corrections to the record and will promptly notify the individual. The System Manager will, if an accounting of disclosure of the record has been made, advise all previous recipients of the record, which was corrected, of the correction and its substance. This will be done in all instances when a record is amended. If, after review, the Board decides that the request for amendment should be denied, it will promptly forward its recommendation to the Director, DCA. A majority vote of the members of the Board will constitute a recommendation to the Director.

(x) The Director, DISA, upon receipt of the Board's recommendation, will complete the review and make a final determination.

(xi) If the Director, DISA, after his review, agrees with the individual's request to amend the record, he will, through the DISA Counsel, so advise the individual in writing. The System Manager will receive a copy of the Director's decision and will assure that the record is corrected accordingly and that if an accounting of disclosure of the record has been made, advise all previous recipients of the record which was corrected of the correction and its substance.

(xii) If, after his review, the Director refuses to amend the records as the individual requested, he will, through the DISA Counsel, advise the individual of his refusal and the reasons for it; of the individual's right to file a concise statement setting forth the reasons for the individual's disagreement with the decision of the Director, DISA; that the statement which is filed will be made available to anyone to whom the record is subsequently disclosed together with, at the discretion of the Agency, a brief statement by the Agency summarizing its reasons for refusing to amend the record; that prior recipients of the disputed record will be provided a copy of any statement of dispute to the extent that an accounting of disclosures was maintained; and of the individual's right to seek judicial review of the Agency's refusal to amend a record.

(xiii) The Director's final determination on the individual's request for a review of the System Manager's initial refusal to amend the record must be concluded within 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requested such review unless the Director determines that a fair and equitable review cannot be made within that time. If additional time is required, the individual will be informed in writing of reasons for the delay and of the approximate date on which the review is expected to be completed.

(xiv) After the Director, DISA has refused to amend a record and the individual has filed a statement setting forth the reasons for the individual's disagreement with the decision of the Director, the System Manager will clearly note any portion of the record which is disputed. The System Manager's notation should make clear that the record is disputed and this should be apparent to anyone who may subsequently have access to, use, or disclose the record. When the System Manager has previously disclosed or will subsequently disclose that portion of the record which is disputed he will note that that portion of the record is disputed and will provide the recipients of the record with a copy of the individual's statement setting forth the reasons for the individual's disagreement with the decision of the Director not to amend the record. The System Manager will also provide recipients of the disputed record with a brief summary of the Director's reasons for not making the requested amendments to the record.

(xv) Nothing herein shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

(xvi) Any requests by an individual for access to or copies of his records shall be processed in accordance with this part and 32 CFR part 310.

(d) DISA System Managers will be:

(1) Responsible for complying with the provisions contained in 32 CFR 310.8 relating to the disclosure to others of personal records, obtaining the written consent of individuals to whom the record pertains, and for keeping an accurate accounting of each disclosure of a record.

(2) Responsible for providing to the Civilian Assistant to the Chief of Staff the information requested in 32 CFR 310.5. However, the information will be reported on a quarterly basis with the first report due to the Civilian Assistant to the Chief of Staff by 31 December 1975.

(e) The Assistant to the Director for Administration, Headquarters, DCA will:

(1) Be responsible for furnishing written guidelines to assist System Managers and other DISA officials in evaluating and implementing paperwork management procedures required under the Privacy Act of 1974. In this regard it should be noted that the Act establishes a number of requirements. Among these are the requirements:

(i) To disclose records contained in a system of records only under conditions specified in the law,

(ii) To maintain an accounting of such disclosures,

(iii) To establish procedures for the disclosure to an individual of his record or information pertaining to him,

(iv) For reviewing a request concerning the amendment of such record, and

(v) For permitting individuals to file a statement of disagreement which will be forwarded with subsequent disclosures.

The guidelines will cover those portions of the Privacy Act which requires paperwork systems for implementation. In preparing those guidelines the Assistant to the Director for Administration will make use of the ''Records Management System for Implementing the Privacy Act'' as provided by the GSA and National Archives and Records Service, Office of Records Management. The GSA and NARA procedures and guidelines will be adapted and modified as required to meet DISA needs.

(2) Be responsible for providing the ''Forms'' which are required to comply with 32 CFR 310.9(b).

(f) The Assistant to the Director for Personnel, Headquarters, DISA will:

(1) Be responsible for development, within DISA, of an appropriate training program for all DISA personnel whose duties involve responsibilities for systems of records affected by the Privacy Act.

(2) Assure that DISA personnel involved in the design, development, operation, or maintenance of any system of records, as defined in 32 CFR 310.6 are informed of all requirements to protect the privacy of the individuals who are subjects of the records. The criminal penalties and civil suit aspects of the Privacy Act will be emphasized.

(3) Assure that within DISA administrative and physical safeguards are established to protect information from 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.

(a) *System identifier and name:* K890.23, DISA Inspector General Investigative Tracker (DIGit).

(1) Exemptions: Any portion of this record system which falls within the provisions of 5 U.S.C. 552a(j)(2), (k)(2)and (k)(5) may be exempt from the following subsections of 5 U.S.C. 552a: (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I).

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

(3) Reasons: To ensure the integrity of the privacy and civil liberties process. The execution requires that information be provided in a free and open manner without fear of retribution or harassment in order to facilitate a just, thorough, and timely resolution of the complaint or inquiry. Disclosures from this system can enable individuals to conceal their wrongdoing or mislead the course of the investigation

by concealing, destroying, or fabricating evidence or documents. In addition, disclosures can subject sources and witnesses to harassment or intimidation which may cause individuals not to seek redress for wrongs through privacy and civil liberties channels for fear of retribution or harassment.

(b) [Reserved]

[42 FR 20298, Apr. 19, 1977. Redesignated at 57 FR 6074, Feb. 20, 1992, as amended at 62 FR 26390, May 14, 1997; 79 FR 64510, Oct. 30, 2014]

PART 317—DCAA PRIVACY ACT PROGRAM

Sec.
317.1 Purpose.
317.2 Applicability and scope.
317.3 Policy.
317.4 Responsibilities.
317.5 Procedures.
317.6 Procedures for exemptions.

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

SOURCE: 80 FR 12559, Mar. 10, 2015, unless otherwise noted.

§ 317.1 Purpose.

This part provides policies and procedures for the Defense Contract Audit Agency's (DCAA) implementation of the Privacy Act of 1974 (5 U.S.C. 552a) and 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 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.

(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 substantial 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.

(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) 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.

(6) 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 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 compliance with this part to assure 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 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).

§ 317.6 Procedures for exemptions.

(a) *General information.* There are two types of exemptions, general and specific. The general exemption authorizes the exemption of a system of records from all but a few requirements of the Privacy Act. The specific exemption authorizes exemption of a system of records or portion thereof, from only a few specific requirements. If a new system of records originates for which an exemption is proposed, or an additional or new exemption for an existing system of records is proposed, the exemption shall be submitted with the system of records notice. No exemption of a system of records shall be considered automatic for all records in the system. The systems manager shall review each requested record and apply the exemptions only when this will serve significant and legitimate Government purposes.

(b) *Specific exemptions.* (1) System identifier and name: RDCAA 900.1, DCAA Internal Review Case Files

(i) Exemption: Any portions of this system of records which fall under the provisions of 5 U.S.C. 552a(k)(2) and (k)(5) may be exempt from the following subsections of 5 U.S.C. 552a: (c)(3), (d), (e)(1), (e)(4)(G), (H), and (f).

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

(iii) Reason: (A) From subsection (c)(3) because disclosures from this system could interfere with the just, thorough and timely resolution of the complaint or inquiry, and possibly enable individuals to conceal their wrongdoing or mislead the course of the investigation by concealing, destroying or fabricating evidence or documents.

(B) From subsection (d) because disclosures from this system could interfere with the just, thorough and timely resolution of the complaint or inquiry, and possibly enable individuals to conceal their wrongdoing or mislead the course of the investigation by concealing, destroying or fabricating evidence or documents. Disclosures could also subject sources and witnesses to harassment or intimidation which jeopardize the safety and well-being of themselves and their families.

(C) From subsection (e)(1) because the nature of the investigation functions creates unique problems in prescribing specific parameters in a particular case as to what information is relevant or necessary. Due to close liaison and working relationships with other Federal, state, local, foreign country law enforcement agencies, and other governmental agencies, information may be received which may relate to a case under the investigative jurisdiction of another government agency. It is necessary to maintain this information in order to provide leads for appropriate law enforcement purposes and to establish patterns of activity which may relate to the jurisdiction of other cooperating agencies.

(D) From subsection (e)(4)(G) through (H) because this system of records is exempt from the access provisions of subsection (d).

(E) From subsection (f) because the agency's rules are inapplicable to those portions of the system that are exempt and would place the burden on the agency of either confirming or denying the existence of a record pertaining to a requesting individual might in itself provide an answer to that individual relating to an on-going investigation. The conduct of a successful investigation leading to the indictment of a criminal offender precludes the applicability of established agency rules relating to verification of record, disclosure of the record to that individual,

and record amendment procedures for this record system.

(2) [Reserved]

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

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

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.

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.

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

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

§ 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).

(d) *System identifier and name:* HDTRA 021, Freedom of Information Act and Privacy Act Request Case Files.

(1) *Exemption:* During the processing of a Freedom of Information Act or Privacy Act request exempt materials from other systems of records may in turn become part of the case record in this system. To the extent that copies of exempt records from those 'other' systems of records are entered into this system, the Defense Threat Reduction Agency claims the same exemptions for the records from those 'other' systems that are entered into this system, as claimed for the original primary system of which they are a part.

(2) *Authority:* 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), (k)(3), (k)(4), (k)(5), (k)(6) and (k)(7).

(3) *Reasons:* Records are only exempt from pertinent provisions of 5 U.S.C. 552a to the extent such provisions have been identified and an exemption claimed for the original record and the purposes underlying the exemption for the original record still pertain to the record which is now contained in this system of records. In general, the exemptions were claimed in order to protect properly classified information relating to national defense and foreign policy, to avoid interference during the conduct of criminal, civil, or administrative actions or investigations, to ensure protective services provided the President and others are not compromised, to protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations, to preserve the confidentiality and integrity of Federal testing materials, and to safeguard evaluation materials used for military promotions when furnished by a confidential source. The exemption rule for the original records will identify the specific reasons why the records are exempt from specific provisions of 5 U.S.C. 552a.

[65 FR 18894, Apr. 10, 2000, as amended at 71 FR 64633, Nov. 3, 2006]

PART 319—DEFENSE INTELLIGENCE AGENCY PRIVACY PROGRAM

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.

(c) The Defense Intelligence Agency may have physical custody of the official records of another Federal agency which exercises dominion and control over the records, their content, and access thereto. In such cases, the Defense Intelligence Agency maintenance of the records is considered subject to the rules of the other Federal agency. Except for a request for a determination of the existence of the record, when the Defense Intelligence Agency receives requests related to these records, the DIA will immediately refer the request to the controlling agency for all decisions regarding the request and will notify the individual making the request of the referral.

(d) Records subject to provisions of the Act which are transferred to the Washington National Records Center for storage shall be considered to be maintained by the Defense Intelligence Agency. Disclosure from such records—to other than an element of the Defense Intelligence Agency—can only be made with the prior approval of the Defense Intelligence Agency.

(e) Records subject to provisions of the act which are transferred to the National Archives shall be considered to be maintained by the National Archives and are no longer records of the Agency.

§ 319.4 Definitions.

(a) All terms used in this part which are defined in 5 U.S.C. 552a shall have the same meaning herein.

(b) As used in this part:

(1) The term *Act* means the Privacy Act of 1974, Pub. L. 93–579, 5 U.S.C. 552a.

(2) The term *Agency* means the Defense Intelligence Agency.

§ 319.5 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 Intelligence 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 encouraged 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 § 319.5 of this part, the individual seeking notification, review or copies, and an accounting of disclosures will provide in writing his or her full name, address, social security account number or date of birth and a telephone number where the requester can be contacted should questions arise concerning his or her 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 of the record system specified and any other system which may contain information concerning the individual. A signed notarized statement 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) A request for medical records must be submitted as set forth in § 319.7, of this part.

(e) Individuals should mail their written request to the Defense Intelligence Agency, DSP–1A, Washington, DC 20340–3299 and indicate clearly on the outer envelope ''Privacy Act Request''.

(f) An individual who makes a request on behalf of a minor or legal incompetent shall provide a signed notarized statement affirming the relationship.

(g) When an individual wishes to authorize another person access to his or her records, the individual shall provide a signed notarized statement authorizing and consenting to access by the designated person.

(h) Except as provided by section 552a(b) of the act, 5 U.S.C. 552a(b), the written request or prior written consent of the individual to whom a record pertains shall be required before such record is disclosed to any person or to another agency outside the Department of Defense.

(i) Any person who knowingly and willfully requests or obtains any record concerning an individual from this Agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

[51 FR 44064, Dec. 8, 1986. Redesignated at 56 FR 56595, Nov. 6, 1991 and 56 FR 57799, Nov. 14, 1991, and amended at 56 FR 56595, Nov. 6, 1991]

§ 319.6 Disclosure of requested information to individuals.

The Defense Intelligence Agency, upon receiving a request for notification of the existence of a record or for access to a record, shall:

(a) Determine whether such record exists;

(b) Determine whether access is available under the Privacy Act;

(c) Notify the requester of those determinations within 10 days (excluding Saturday, Sunday and legal public holidays); and

(d) Provide access to information pertaining to that person which has been determined to be available.

§ 319.7 Special procedures: Medical records.

Medical records, requested pursuant to § 319.5 of this part, will be disclosed to the requester unless the disclosure of such records directly to the requester could, in the judgment of a physician, have an adverse effect on the physical or mental health or safety and welfare of the requester or other persons with whom he may have contact. In such an instance, the information will be transmitted to a physician named by the requester or to a person qualified to make a psychiatric or medical determination.

[51 FR 44064, Dec. 8, 1986. Redesignated at 56 FR 56595, Nov. 6, 1991 and 56 FR 57799, Nov. 14, 1991, and amended at 56 FR 56595, Nov. 6, 1991]

§ 319.8 Request for correction or amendment to record.

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

(b) Such requests shall be in writing and may be mailed to DSP–1A as indicated in § 319.5.

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

[51 FR 44064, Dec. 8, 1986. Redesignated at 56 FR 56595, Nov. 6, 1991 and 56 FR 57799, Nov. 14, 1991, and amended at 56 FR 56595, Nov. 6, 1991]

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

(a) The Agency will acknowledge a request for correction or amendment of a record within 10 days (excluding Saturday, Sunday, and legal public holidays) 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 days (excluding Saturday, Sunday, and legal holidays) 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.

§ 319.10 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 to 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 should be in writing and may be mailed to RTS–1 as indicated in § 319.5.

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

(d) Within 30 days (excluding Saturday, Sunday, and legal public holidays) of the receipt of request for review, the Agency shall advise the individual of the final disposition of his or her 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 determinations are 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 with record in question a concise statement of his or her reasons for disagreeing with the Agency's decision,

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

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

[51 FR 44064, Dec. 8, 1986. Redesignated at 56 FR 56595, Nov. 6, 1991 and 56 FR 57799, Nov. 14, 1991, and amended at 56 FR 56595, Nov. 6, 1991]

§ 319.11 Fees.

(a) The schedule of fees chargeable is contained at § 286.60 *et seq*. As a component of the Department of Defense, the applicable published Departmental rules and schedules with respect to fees will also be the policy of DIA.

(b) Current employees of the Agency will not be charged for the first copy of a record provided by the Agency.

(c) In the absence of an agreement to pay required anticipated costs, the time for responding to a request begins on resolution of this agreement to pay.

(d) The fees may be paid by check, draft or postal money order payable to the Treasurer of the United States. Remittance will be forwarded to the office designated in § 319.5(e).

[51 FR 44064, Dec. 8, 1986. Redesignated at 56 FR 56595, Nov. 6, 1991 and 56 FR 57799, Nov. 14, 1991, and amended at 56 FR 56595, Nov. 6, 1991]

§ 319.12 General exemptions. [Reserved]

§ 319.13 Specific exemptions.

(a) All systems of records maintained by the Director Intelligence Agency shall be exempt from the requirements of 5 U.S.C. 552a(d) pursuant to 5 U.S.C. 552a(k)(1) to the extent that the system contains any information properly classified under 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 specifically designated for exemption may contain isolated information which has been properly classified.

(b) The Director, Defense Intelligence Agency, designated the systems of records listed below for exemptions under the specified provisions of the Privacy Act of 1974, as amended (Pub. L. 93–579):

(c) *System identification and name:* LDIA 0271, Investigations and Complaints.

(1) *Exemption:* Any portion of this record system which falls within the provisions of 5 U.S.C. 552a(k) (2) and (5) may be exempt from the following subsections of 5 U.S.C. 552a: (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (e)(4)(I).

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

(3) *Reasons:* The reasons for asserting these exemptions are to ensure the integrity of the Inspector General process within the Agency. The execution requires that information be provided in a free and open manner without fear of retribution or harassment in order to facilitate a just, thorough and timely resolution of the complaint or inquiry. Disclosures from this system can enable individuals to conceal their wrongdoing or mislead the course of the investigation by concealing, destroying or fabricating evidence or documents. Also, disclosures can subject sources and witnesses to harassment or intimidation which may cause individuals not to seek redress for wrongs through Inspector General channels for fear of retribution or harassment.

(d) *System identifier and name:* LDIA 13–0001, Conflict Management Programs.

(1) *Exemptions:* Any portion of this record system which falls within the provisions of 5 U.S.C. 552a(k)(2) and (k)(5) may be exempt from the following subsections of 5 U.S.C. 552a: (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I)

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

(3) *Reasons:* Claiming these exemptions ensures the integrity of the conflict management process. The execution requires that information be provided in a free and open manner without fear of retribution or harassment

in order to facilitate a just, thorough, and timely resolution of the complaint or inquiry. Disclosures from this system can enable individuals to conceal their wrongdoing or mislead the course of the investigation by concealing, destroying, or fabricating evidence or documents. In addition, disclosures can subject sources and witnesses to harassment or intimidation which may cause individuals to not seek redress for wrongs through available channels for fear of retribution or harassment.

(e) *System identifier and name:* LDIA 0660, Security and Counterintelligence Files.

(1) *Exemption:* Any portion of this record system which falls within the provisions of 5 U.S.C. 552a(k)(2), (k)(5) and (k)(6) may be exempt from the following subsections of 5 U.S.C. 552a: (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (e)(4)(I).

(2) *Authority:* 5 U.S.C. 552a(k)(2), (k)(5) and (k)(6).

(3) *Reasons:* The reasons for asserting these exemptions are to ensure the integrity of the adjudication process used by the Agency to determine the suitability, eligibility or qualification for Federal service with the Agency and to make determinations concerning the questions of access to classified materials and activities. The proper execution of this function requires that the Agency have the ability to obtain candid and necessary information in order to fully develop or resolve pertinent information developed in the process. Potential sources, out of fear or retaliation, exposure or other action, may be unwilling to provide needed information or may not be sufficiently frank to be a value in personnel screening, thereby seriously interfering with the proper conduct and adjudication of such matters; and protects information used for medical, psychological evaluations, security questionnaires and polygraph testing.

(f) [Reserved]

(g) *System identifier and name:* LDIA 10–0001, Equal Opportunity, Diversity and Alternate Dispute Resolution Records.

(1) *Exemption:* Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identity of a confidential source. NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

The specific sections of 5 U.S.C. 552a from which the system is to be exempted are 5 U.S.C. 552a (c)(3) and (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (H), and (I), (e)(5), (f), and (g).

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

(3) *Reasons:* (i) From subsection (c)(3) because to grant access to an accounting of disclosures as required by the Privacy Act, including the date, nature, and purpose of each disclosure and the identity of the recipient, could alert the subject to the existence of the investigation or prospective interest by DIA or other agencies. This could seriously compromise case preparation by prematurely revealing its existence and nature; compromise or interfere with witnesses or make witnesses reluctant to cooperate; and lead to suppression, alteration, or destruction of evidence.

(ii) From subsections (c)(4), (d), and (f) because providing access to this information could result in the concealment, destruction or fabrication of evidence and jeopardize the safety and well being of informants, witnesses and their families, and law enforcement personnel and their families. Disclosure of this information could also reveal and render ineffectual investigative techniques, sources, and methods used by this component and could result in the invasion of privacy of individuals only incidentally related to an investigation. Investigatory material is exempt to the extent that the disclosure of such material would reveal the identity of a source who furnished the information to the Government under an express promise that the identity of the source would be held in confidence, or prior to September 27, 1975 under an

implied promise that the identity of the source would be held in confidence. This exemption will protect the identities of certain sources that would be otherwise unwilling to provide information to the Government. The exemption of the individual's right of access to his/her records and the reasons therefore necessitate the exemptions of this system of records from the requirements of the other cited provisions.

(iii) From subsection (e)(1) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsection (e)(2) because collecting information to the fullest extent possible directly from the subject individual may or may not be practical in a criminal investigation.

(v) From subsection (e)(3) because supplying an individual with a form containing a Privacy Act Statement would tend to inhibit cooperation by many individuals involved in a criminal investigation. The effect would be somewhat adverse to established investigative methods and techniques.

(vi) From subsections (e)(4)(G), (H), and (I) because it will provide protection against notification of investigatory material 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). In addition, this system of records is exempt from the access provisions of subsection (d).

(vii) From subsection (e)(5) because the requirement that records be maintained with attention to accuracy, relevance, timeliness, and completeness would unfairly hamper the investigative process. It is the nature of law enforcement for investigations to uncover the commission of illegal acts at diverse stages. It is frequently impossible to determine initially what information is accurate, relevant, timely, and least of all complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light.

(viii) From subsection (f) because the agency's rules are inapplicable to those portions of the system that are exempt and would place the burden on the agency of either confirming or denying the existence of a record pertaining to a requesting individual might in itself provide an answer to that individual relating to an on-going investigation. The conduct of a successful investigation leading to the indictment of a criminal offender precludes the applicability of established agency rules relating to verification of record, disclosure of the record to the individual and record amendment procedures for this record system.

(ix) From subsection (g) because this system of records should be exempt to the extent that the civil remedies relate to provisions of 5 U.S.C. 552a from which this rule exempts the system.

(h) *System identifier and name:* LDIA 10–0002, Foreign Intelligence and Counterintelligence Operation Records.

(1) *Exemption:* (i) Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identity of a confidential source. NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(ii) The specific sections of 5 U.S.C. 552a from which the system is to be exempted are 5 U.S.C. 552a (c)(3) and (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (H), and (I), (e)(5), (f), and (g).

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

(3) *Reasons:* (i) From subsection (c)(3) because to grant access to an accounting of disclosures as required by the Privacy Act, including the date, nature, and purpose of each disclosure and the identity of the recipient, could alert the subject to the existence of the investigation or prospective interest by DIA or other agencies. This could seriously compromise case preparation by prematurely revealing its existence and nature; compromise or interfere with witnesses or make witnesses reluctant to cooperate; and lead to suppression, alteration, or destruction of evidence.

(ii) From subsections (c)(4), (d), and (f) because providing access to this information could result in the concealment, destruction or fabrication of evidence and jeopardize the safety and well being of informants, witnesses and their families, and law enforcement personnel and their families. Disclosure of this information could also reveal and render ineffectual investigative techniques, sources, and methods used by this component and could result in the invasion of privacy of individuals only incidentally related to an investigation. Investigatory material is exempt to the extent that the disclosure of such material would reveal the identity of a source who furnished the information to the Government under an express promise that the identity of the source would be held in confidence, or prior to September 27, 1975 under an implied promise that the identity of the source would be held in confidence. This exemption will protect the identities of certain sources that would be otherwise unwilling to provide information to the Government. The exemption of the individual's right of access to his/her records and the reasons therefore necessitate the exemptions of this system of records from the requirements of the other cited provisions.

(iii) From subsection (e)(1) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsection (e)(2) because collecting information to the fullest extent possible directly from the subject individual may or may not be practical in a criminal investigation.

(v) From subsection (e)(3) because supplying an individual with a form containing a Privacy Act Statement would tend to inhibit cooperation by many individuals involved in a criminal investigation. The effect would be somewhat adverse to established investigative methods and techniques.

(vi) From subsections (e)(4)(G), (H), and (I) because it will provide protection against notification of investigatory material 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). In addition, this system of records is exempt from the access provisions of subsection (d).

(vii) From subsection (e)(5) because the requirement that records be maintained with attention to accuracy, relevance, timeliness, and completeness would unfairly hamper the investigative process. It is the nature of law enforcement for investigations to uncover the commission of illegal acts at diverse stages. It is frequently impossible to determine initially what information is accurate, relevant, timely, and least of all complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light.

(viii) From subsection (f) because the agency's rules are inapplicable to those portions of the system that are exempt and would place the burden on the agency of either confirming or denying the existence of a record pertaining to a requesting individual might in itself provide an answer to that individual relating to an on-going investigation. The conduct of a successful investigation leading to the indictment of a

criminal offender precludes the applicability of established agency rules relating to verification of record, disclosure of the record to the individual and record amendment procedures for this record system.

(ix) From subsection (g) because this system of records should be exempt to the extent that the civil remedies relate to provisions of 5 U.S.C. 552a from which this rule exempts the system.

(i) *System identifier and name:* LDIA 0900, Accounts Receivable, Indebtedness and Claims.

(1) *Exemption:* During the course of accounts receivable, indebtedness or claims actions, exempt materials from other systems of records may in turn become part of the case record in this system. To the extent that copies of exempt records from those ''other'' systems of records are entered into this system, the DIA hereby claims the same exemptions for the records from those ''other'' systems that are entered into this system, as claimed for the original primary system of which they are a part.

(2) *Authority:* 5 U.S.C. 552a(k)(2) through (k)(7).

(3) *Reasons:* Records are only exempt from pertinent provisions of 5 U.S.C. 552a to the extent such provisions have been identified and an exemption claimed for the original record and the purposes underlying the exemption for the original record still pertain to the record which is now contained in this system of records. In general, the exemptions were claimed in order to protect properly classified information relating to national defense and foreign policy, to avoid interference during the conduct of criminal, civil, or administrative actions or investigations, to ensure protective services provided the President and others are not compromised, to protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations, to preserve the confidentiality and integrity of Federal testing materials, and to safeguard evaluation materials used for military promotions when furnished by a confidential source. The exemption rule for the original records will identify the specific reasons why the records are exempt from specific provisions of 5 U.S.C. 552a.

(j) *System identifier and name:* LDIA 0010, Information Requests-Freedom of Information Act (FOIA) and Privacy Act.

(1) *Exemption:* During the course of information requests-FOIA and Privacy Act actions, exempt records/material from other systems of records may become part of this system of records. For such records/material, DIA hereby claims the same exemptions as is claimed for the systems from which such records/material are derived.

(2) *Authority:* 5 U.S.C. 552a(k)(2) through (k)(7).

(3) *Reasons:* Records in a system of records are only exempted from pertinent provisions of 5 U.S.C. 552a to the extent such provisions are identified and an exemption claimed. In general, exemptions claimed protect properly classified information relating to national defense and foreign policy; avoid interference during the conduct of criminal, civil, or administrative actions or investigations; ensure protective services provided the President and others are not compromised; protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations; preserve the confidentiality and integrity of Federal testing materials; and safeguard evaluation materials used for military promotions when furnished by a confidential source. The exemption rule(s) for the systems of records from which the records/materials was derived will identify the specific reasons why the records/materials are exempt from provisions of 5 U.S.C. 552a.

(k) *System identifier and name:* LDIA 12–0002, Privacy and Civil Liberties Case Management System.

(1) *Exemptions:* Any portion of this record system which falls within the provisions of 5 U.S.C. 552a(k)(2)and (k)(5) may be exempt from the following subsections of 5 U.S.C. 552a: (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I).

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

(3) The reasons for asserting these exemptions is to ensure the integrity of the privacy and civil liberties process.

The execution requires that information be provided in a free and open manner without fear of retribution or harassment in order to facilitate a just, thorough, and timely resolution of the complaint or inquiry. Disclosures from this system can enable individuals to conceal their wrongdoing or mislead the course of the investigation by concealing, destroying, or fabricating evidence or documents. In addition, disclosures can subject sources and witnesses to harassment or intimidation which may cause individuals not to seek redress for wrongs through privacy and civil liberties channels for fear of retribution or harassment.

(l) *System identifier and name:* LDIA 0209, Litigation Case Files.

(1) *Exemptions:* Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C 552a(j)(2), may be exempt pursuant to 5 U.S.C 552(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or which he would otherwise be eligible, as a result of maintenance of the information, the individual will be provided access to the information except to the extent that disclosure would reveal the identity of a confidential source. This exemption provides limited protection of investigative reports maintained in a system of records used in personnel or administrative actions. Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source. Any portion of this record system which falls within the provisions of 5 U.S.C. 552a(k)(2)and (k)(5) may be exempt from the following subsections of 5 U.S.C. 552a: (c)(3), (d)(1)(2)(3)(4)(5), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I). Exempt materials from other systems of records may in turn become part of the case records in this system. To the extent that copies of exempt records from those 'other' systems of records are entered into this case record, the Defense Intelligence Agency hereby claims the same exemptions for the records from those 'other' systems that are entered into this system, as claimed for the original primary systems of records, which they are a part.

(2) *Authority:* 5 U.S.C. 552a(j)(2), (k)(2), (k)(3), (k)(4), (k)(5), (k)(6), and (k)(7).

(3) *Reasons:* The reason for asserting these exemptions (k)(2) and (k)(5) is to ensure the integrity of the litigation process.

(m) *System identifier and name:* LDIA 10–0004 Occupational, Safety, Health, and Environmental Management Records.

(1) *Exemptions:* Any portion of this record system which falls within the provisions of 5 U.S.C. 552a(k)(2)(k)(4) and (k)(5) may be exempt from the following subsections of 5 U.S.C. 552a: (c)(3); (d)(1), (d)(2), (d)(3), (d)(4), (d)(5); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); (f)(1), (f)(2), (f)(2), (f)(3), (f)(4), (f)(5).

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

(3) The reasons for asserting these exemptions are to ensure the integrity of an investigative or administrative process and to protect statistical records. The execution requires that information be provided in a free and open manner without fear of retribution or harassment in order to facilitate a just, thorough, and timely resolution during an investigation or administrative action. Disclosures from this system can enable individuals to conceal their wrongdoing or mislead the course of the investigation by concealing, destroying, or fabricating evidence or documents. In addition, disclosures can subject sources and witnesses to harassment or intimidation which may cause individuals to not to seek redress for concerns about occupational safety, health, environmental issues and accident reporting. Information is used to comply regulatory reporting requirements.

[56 FR 56595, Nov. 6, 1991, as amended at 76 FR 49659, Aug. 11, 2011; 77 FR 15591, Mar. 16, 2012; 77 FR 57014, 57016, Sept. 17, 2012; 78 FR 69551, 69552, Nov. 20, 2013;]

PART 320—NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY (NGA) PRIVACY

AUTHORITY: Pub. L. 93–579, 88 Stat. 1986 (5 U.S.C. 552a).

SOURCE: 66 FR 52681, Oct. 17, 2001, unless otherwise noted.

EDITORIAL NOTE: Nomenclature changes to part 320 appear at 69 FR 2066, Jan. 14, 2004.

§ 320.1 Purpose and scope.

(a) This part is published pursuant to the Privacy Act of 1974, as amended (5 U.S.C. 552a), (hereinafter the ''Privacy Act''). This part:

(1) Establishes or advises of the procedures whereby an individual can:

(i) Request notification of whether the National Geospatial-Intelligence Agency (NGA) maintains or has disclosed a record pertaining to him in any nonexempt system of records,

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

(iii) Request that the record be amended and

(iv) Appeal any initial adverse determination of any such request;

(2) Specifies those systems of records which the Director, Headquarters NGA has determined to be exempt from the procedures established by this regulation and from certain provisions of the Privacy Act. NGA policy encompasses the safeguarding of individual privacy from any misuse of NGA records and the provision of the fullest access practicable to individuals to NGA records concerning them.

§ 320.2 Definitions.

As used in this part:

(a) *Appellate authority (AA).* A NGA employee who has been granted authority to review the decision of the Initial Denial Authority (IDA) that has been appealed by the Privacy Act requester and make the appeal determination for NGA on the release ability of the records in question.

(b) *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''.

(c) *Initial denial authority (IDA).* A NGA employee, or designee, who has been granted authority to make an initial determination for NGA that records requested in a Privacy Act request should be withheld from disclosure or release.

(d) *Maintain.* Includes maintain, collect, use or disseminate.

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

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

(g) *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.

(h) *System of records.* A group of records under the control of NGA from which personal information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to the individual.

(i) *System manger.* The NGA official who is responsible for the operation and management of a system of records.

§ 320.3 Responsibilities.

(a) Director of NGA:

(1) Implements the NGA privacy program.

(2) Designates the Director of the Public Affairs Office as the NGA Initial Denial Authority;

(3) Designates the Chief of Staff as the Appellate Authority.

(4) Designates the General Counsel as the NGA Privacy Act Officer and the principal point of contact for matters involving the NGA privacy program.

(b) NIMA General Counsel:

(1) Oversees systems of records maintained throughout NIMA, administered by Information Services. This includes coordinating all notices of new systems of records and changes to existing systems for publication in the FEDERAL REGISTER.

(2) Coordinates all denials of requests for access to or amendment of records.

(3) Assesses and collects fees for costs associated with processing Privacy Act requests and approves or denies requests for fee waivers. Fees collected are forwarded through Financial Management Directorate to the U.S. Treasury.

(4) Prepares the annual report to the Defense Privacy Office.

(5) Oversees investigations of allegations of unauthorized maintenance, disclosure, or destruction of records.

(6) Conducts or coordinates Privacy Act training for NGA personnel as needed, including training for public affairs officers and others who deal with the public and news media.

(c) NIMA System Managers:

(1) Ensure that all personnel who either have access to a system of records or who are engaged in developing or supervising procedures for handling records in a system of records are aware of their responsibilities for protecting personal information.

(2) Prepare notices of new systems of records and changes to existing systems for publication in the FEDERAL REGISTER.

(3) Ensure that no records subject to this part are maintained for which a systems notice has not been published.

(4) Respond to requests by individuals for access, correction, or amendment to records maintained pursuant to the NGA privacy program.

(5) Provide recommendations to General Counsel for responses to requests from individuals for access, correction, or amendment to records.

(6) Safeguard records to ensure that they are protected from unauthorized alteration or disclosure.

(7) Dispose of records in accordance with accepted records management practices to prevent inadvertent compromise. Disposal methods such as tearing, burning, melting, chemical decomposition, pulping, pulverizing, shredding, or mutilation are considered adequate if the personal data is rendered unrecognizable or beyond reconstruction.

§ 320.4 Procedures for requesting information.

(a) Upon request in person or by mail, any individual, as defined in § 320.2, shall be informed whether or not any NGA system of records contains a record pertaining to him.

(b) Any individual requesting such information in person may appear at NGA General Counsel Office (refer to the NGA address list at paragraph (e) of this section) or at the NGA office thought to maintain the record in question and shall provide:

(1) Information sufficient to identify the record, e.g., the individual's own name, date of birth, place of birth, and, if possible, an indication of the type of record believed to contain information concerning the individual, and

(2) Acceptable identification to verify the individual's identity, e.g., driver's license, employee identification card or Medicare card.

(c) Any individual requesting such information by mail shall address the request to the Office of General Counsel (refer to paragraph (e) of this section)

or NGA office thought to maintain the record in question and shall include in such request the following:

(1) Information sufficient to identify the record, e.g., the individual's own name, date of birth, place of birth, and, if possible, an indication of the type of record believed to contain information concerning the individual, and

(2) A notarized statement or unsworn declaration in accordance with 28 U.S.C. 1746 to verify the individual's identity, if, in the opinion of the NGA system manager, the sensitivity of the material involved warrants.

(d) NGA procedures on requests for information. Upon receipt of a request for information made in accordance with these regulations, notice of the existence or nonexistence of any records described in such requests will be furnished to the requesting party within ten working days of receipt.

(e) Written requests for access to records should be sent to NGA Bethesda, ATTN: NGA/GC, Mail Stop D–10, 4600 Sangamore Road, Bethesda, MD 20816–5003.

(f) Requests for information made under the Freedom of Information Act are processed in accordance with ''DoD Freedom of Information Act Program Regulation'' (32 CFR part 286).

(g) Requests for personal information from the Government Accounting Office (GAO) are processed in accordance with DoD Directive 7650.1[1] ''GAO Access to Records''.

§ 320.5 Disclosure of requested information.

(a) Upon request by an individual made in accordance with the procedures set forth in this section, such individual shall be granted access to any pertinent record which is contained in a nonexempt NGA system of records. However, nothing in this section shall allow an individual access to any information compiled by NGA in reasonable anticipation of a civil or criminal action or proceeding.

(b) Procedures for requests for access to records. Any individual may request access to a pertinent NGA record in person or by mail.

(1) Any individual making such request in person shall appear at Office of General Counsel, NGA Bethesda, ATTN: NGA/GC, Mail Stop D–10, 4600 Sangamore Road, Bethesda, MD 20816–5003, and shall provide identification to verify the individuals' identity, e.g., driver's license, employee identification card, or Medicare card.

(2) Any individual making a request for access to records by mail shall address such request to the Office of General Counsel, NGA Bethesda, ATTN: NGA/GC, Mail Stop D–10, 4600 Sangamore Road, Bethesda, MD 20816–5003; and shall include therein a signed, notarized statement, or an unsworn statement or declaration in accordance with 28 U.S.C. 1746, to verify identity.

(3) Any individual requesting access to records under this section in person may be accompanied by a person of the individual's own choosing while reviewing the record requested. If an individual elects to be so accompanied, said individual shall give notice of such election in the request and shall provide a written statement authorizing disclosure of the record in the presence of the accompanying person. Failure to so notify NGA in a request for access shall be deemed to be a decision by the individual not to be accompanied.

(c) NGA determination of requests for access.

(1) Upon receipt of a request made in accordance with this section, the NGA Office of General Counsel or NGA office having responsibility for maintenance of the record in question shall release the record, or refer it to an Initial Denial Authority, who shall:

(i) Determine whether such request shall be granted.

(ii) Make such determination and provide notification within 30 working days after receipt of such request.

(iii) Notify the individual that fees for reproducing copies of records will be assessed and should be remitted before the copies may be delivered. Fee schedule and rules for assessing fees are contained in § 320.9.

(iv) Requests for access to personal records may be denied only by an agency official authorized to act as an Initial Denial Authority or Final Denial Authority, after coordination with the Office of General Counsel.

[1] Copies may be obtained via Internet at *http://www.dtic.mil/whs/directives.*

(2) If access to a record is denied because such information has been compiled by NGA in reasonable anticipation of a civil or criminal action or proceeding, the individual will be notified of such determination and his right to judicial appeal under 5 U.S.C. 552a(g).

(d) Manner of providing access.

(1) If access is granted, the individual making the request shall notify NGA whether the records requested are to be copied and mailed.

(2) If the records are to be made available for personal inspection the individual shall arrange for a mutually agreeable time and place for inspection of the record. NIMA reserves the right to require the presence of a NIMA officer or employee during personal inspection of any record pursuant to this section and to request of the individual that a signed acknowledgment of the fact be provided that access to the record in question was granted by NIMA.

§ 320.6 Request for correction or amendment to record.

(a) Any individual may request amendment of a record pertaining to said individual.

(b) After inspection of a pertinent record, the individual may file a request in writing with the NGA Office of General Counsel for amendment. Such requests shall specify the particular portions of the record to be amended, the desired amendments and the reasons, supported by documentary proof, if available.

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

(a) Not later than 10 working days after receipt of a request to amend a record, in whole or in part, the NGA Office of General Counsel, or NGA office having responsibility for maintenance of the record in question, shall correct any portion of the record which the individual demonstrates is not accurate, relevant, timely or complete, and thereafter either inform the individual of such correction or process the request for denial.

(b) Denials of requests for amendment of a record will be made only by an agency official authorized to act as an Initial Denial Authority, after coordination with the Office of General Counsel. The denial letter will inform the individual of the denial to amend the record setting forth the reasons therefor and notifying the individual of his right to appeal the decision to NGA.

(c) Any person or other agency to whom the record has been previously disclosed shall be informed of any correction or notation of dispute with respect to such records.

(d) These provisions for amending records are not intended to permit the alteration of evidence previously presented during any administrative or quasi-judicial proceeding, such as an employee grievance case. Any changes in such records should be made only through the established procedures for such cases. Further, these provisions are not designed to permit collateral attack upon what has already been the subject of an administrative or quasi-judicial action. For example, an individual may not use this procedure to challenge the final decision on a grievance, but the individual would be able to challenge the fact that such action has been incorrectly recorded in his file.

§ 320.8 Appeal of initial adverse agency determination on correction or amendment.

(a) An individual whose request for amendment of a record pertaining to him may further request a review of such determination in accordance with this section.

(b) Not later than 30 working days following receipt of notification of denial to amend, an individual may file an appeal of such decision with NGA. The appeal shall be in writing, mailed or delivered to NGA, ATTN: Mail Stop D–10, 4600 Sangamore Road, Bethesda, MD 20816–5003. The appeal must identify the records involved, indicate the dates of the request and adverse determination, and indicate the express basis for that determination. In addition, the letter of appeal shall state briefly and succinctly the reasons why the adverse determination should be reversed.

(c) Upon appeal from a denial to amend a record the NGA Appellate Authority or designee shall make a determination whether to amend the record and must notify the individual of that determination by mail, not later than 10 working days after receipt of such appeal, unless extended pursuant to paragraph (d) of this section.

(1) The Appellate Authority or designee shall also notify the individual of the provisions of the Privacy Act of 1974 regarding judicial review of the NGA Appellate Authority's determination.

(2) If on appeal the denial to amend the record is upheld, the individual shall be permitted to file a statement setting forth the reasons for disagreement with the Appellate Authority's determination and such statement shall be appended to the record in question.

(d) The Appellate Authority or designee may extend up to 30 days the time period in which to make a determination on an appeal from denial to amend a record for the reason that a fair and equitable review cannot be completed within the prescribed time period.

§ 320.9 Disclosure of record to person other than the individual to whom it pertains.

(a) No officer or employee of NGA will disclose any record which is contained in a system of records, by any means of communication to any person or agency within or outside the Department of Defense without the request or consent of the individual to whom the record pertains, except as described in to 32 CFR 310.41; Appendix C to part 310 of this chapter; and/or a NGA Privacy Act system of records notice.

(b) Any such record may be disclosed to any person or other agency only upon written request, of the individual to whom the record pertains.

(c) In the absence of a written consent from the individual to whom the record pertains, such record may be disclosed only provided such disclosure is:

(1) To those officers and employees of the DoD who have a need for the record in the performance of their duties.

(2) Required under the Freedom of Information Act (32 CFR part 286).

(3) For a routine use established within the system of records notice.

(4) To the Bureau of Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13.

(5) To a recipient who has provided the NGA with adequate advance written assurance that the record will be used solely as a statistical research or reporting record and the record is transferred in a form that is not individually identifiable and will not be used to make any decisions about the rights, benefits or entitlements of an individual.

(6) To the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the U.S. Government or for evaluation by the Administrator of the General Services Administration or his designee to determine whether the record has such value.

(7) To another agency or to an instrumentality of any governmental jurisdiction within or under the control of the U.S. for a civil or criminal law enforcement activity authorized by law, provided the head of the agency or instrumentality has made a prior written request to the Director, NGA specifying the particular record and the law enforcement activity for which it is sought.

(8) To a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual, if upon such disclosure notification is transmitted to the last known address of such individual.

(9) To either house of Congress, and, to the extent of the matter within its jurisdiction, any committee or subcommittee or joint committee of Congress.

(10) To the Comptroller General or any of his authorized representatives in the course of the performance of the duties of the GAO.

(11) Under an order of a court of competent jurisdiction.

(12) To a consumer reporting agency in accordance with section 3711(f) of title 31.

(d) Except for disclosures made pursuant to paragraphs (c)(1) and (2) of this section, an accurate accounting will be kept of the data, nature and purpose of each disclosure of a record to any person or agency, and the name and address of the person or agency to whom the disclosure was made. The accounting of disclosures will be made available for review by the subject of a record at his request except for disclosures made pursuant to paragraph (c)(7) of this section. If an accounting of disclosure has been made, any person or agency contained therein will be informed of any correction or notation of dispute made pursuant to section 320.6 of this part.

§ 320.10 Fees.

Individuals may request copies for retention of any documents to which they are granted access to NGA 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.

§ 320.11 Penalties.

The Privacy Act of 1974 (5 U.S.C. 552a(i)(3)) makes it a misdemeanor subject to a maximum fine of $5,000, to knowingly and willfully request or obtain any record concerning an individual under false pretenses. The Act also establishes similar penalties for violations by NGA employees of the Act or regulations established thereunder.

§ 320.12 Exemptions.

(a) *Exempt systems of record.* All systems of records maintained by the NGA and its components shall be exempt from the requirements of 5 U.S.C. 552a(d) pursuant to 5 U.S.C. 552a(k)(1) to the extent that the system contains any information properly classified under Executive Order 12958 and that is required by Executive Order to be withheld 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:* B0210–07, Inspector General Investigative and Complaint Files.

(1) *Exemptions:* (i) Investigative material compiled for law enforcement purposes may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source.

(ii) Investigative material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(iii) Therefore, portions of this system of records may be exempt pursuant to 5 U.S.C. 552a(k)(2) and/or (k)(5) from the following subsections of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H) and (I), and (f).

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

(3) *Reasons:* (i) From subsection (c)(3) because to grant access to the accounting for each disclosure as required by the Privacy Act, including the date, nature, and purpose of each disclosure and the identity of the recipient, could alert the subject to the existence of the investigation or prosecutable interest by the NGA or other agencies. This could seriously compromise case preparation by prematurely revealing its existence and nature; compromise or interfere with witnesses or make witnesses reluctant to cooperate; and lead to suppression, alteration, or destruction of evidence.

(ii) From subsections (d) and (f) because providing access to investigative records 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; enable individuals to conceal their wrongdoing or mislead the course of the investigation; 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) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because this system of records is compiled for investigative purposes and is exempt from the access provisions of subsections (d) and (f).

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NGA will, nevertheless, continue to publish such a notice in broad generic terms, as is its current practice.

(vi) Consistent with the legislative purpose of the Privacy Act of 1974, NGA will grant access to nonexempt material in the records being maintained. Disclosure will be governed by NGA's Privacy Regulation, but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal or civil violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered; the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of the above nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated in this paragraph. The decisions to release information from these systems will be made on a case-by-case basis.

(c) *System identifier and name:* NGA–004, NGA Threat Mitigation Records. (1) *Exemptions:* Exempt materials from JUSTICE/FBI—019 Terrorist Screening Records System may become part of the case records in this system of records. To the extent that copies of exempt records from JUSTICE/FBI—019, Terrorist Screening Records System are entered into these Threat Mitigation case records, NGA hereby claims the same exemptions (j)(2) and (k)(2), for the records as claimed in JUSTICE/FBI—019, Terrorist Screening Records system of records of which they are a part.

(2) Information specifically authorized to be classified under E.O. 12958, as implemented by DoD 5200.1–R, may be exempt pursuant to 5 U.S.C. 552a(k)(1).

(3) Investigative material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(4) *Authority:* 5 U.S.C. 552a(j)(2), (k)(1), (k)(2) and (k)(5).

(5) *Reasons:* (i) Pursuant to *5 U.S.C. 552a(j)(2),* (k)(2), and (k)(5) NGA is claiming the following exemptions for certain records within the Threat Mitigation Records system: *5 U.S.C. 552a(c)(3)* and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (5), and (8); (f), and (g). Additionally, pursuant to 5 U.S.C. 552a(k)(1) and (k)(2), NGA has exempted this system from the following provisions of the Privacy Act, subject to the limitation set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). Exemptions from these particular subsections are justified, on a case-by-case basis to be

determined at the time a request is made.

(ii) In addition to records under the control of NGA, the Threat Mitigation system of records may include records originating from systems of records of other law enforcement and intelligence agencies which may be exempt from certain provisions of the Privacy Act. However, NGA does not assert exemption to any provisions of the Privacy Act with respect to information submitted by or on behalf of individuals.

(iii) To the extent the Threat Mitigation system contains records originating from other systems of records, NGA will rely on the exemptions claimed for those records in the originating system of records. Exemptions for certain records within the Threat Mitigation system from particular subsections of the Privacy Act are justified for the following reasons:

(A) From subsection (c)(3) (Accounting for Disclosures) because giving a record subject access to the accounting of disclosures from records concerning him or her could reveal investigative interest on the part of the recipient agency that obtained the record pursuant to a routine use. Disclosure of the accounting could therefore present a serious impediment to law enforcement efforts on the part of the recipient agency because the individual who is the subject of the record would learn of third agency investigative interests and could take steps to evade detection or apprehension. Disclosure of the accounting also could reveal the details of watch list matching measures under the Threat Mitigation system, as well as capabilities and vulnerabilities of the watch list matching process, the release of which could permit an individual to evade future detection and thereby impede efforts to ensure security.

(B) From subsection (c)(4) because portions of this system are exempt from the access and amendment provisions of subsection (d).

(C) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of Department of Homeland Security or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to national security.

(D) From subsection (e)(1) because it is not always possible for NGA or other agencies to know in advance what information is both relevant and necessary for it to complete an identity comparison between individuals and a known or suspected terrorist. In addition, because NGA and other agencies may not always know what information about an encounter with a known or suspected terrorist will be relevant to law enforcement for the purpose of conducting an operational response.

(E) From subsection (e)(2) because application of this provision could present a serious impediment to counterterrorism, law enforcement, or intelligence efforts in that it would put the subject of an investigation, study or analysis on notice of that fact, thereby permitting the subject to engage in conduct designed to frustrate or impede that activity. The nature of counterterrorism, law enforcement, or intelligence investigations is such that vital information about an individual frequently can be obtained only from other persons who are familiar with such individual and his/her activities. In such investigations, it is not feasible to rely upon information furnished by the individual concerning his own activities.

(F) From subsection (e)(3), to the extent that this subsection is interpreted to require NGA to provide notice to an individual if NGA or another agency receives or collects information about that individual during an investigation or from a third party. Should the subsection be so interpreted, exemption

from this provision is necessary to avoid impeding counterterrorism, law enforcement, or intelligence efforts by putting the subject of an investigation, study or analysis on notice of that fact, thereby permitting the subject to engage in conduct intended to frustrate or impede that activity.

(G) From subsections (e)(4)(G) and (H) and (I) (Agency Requirements) and (f) (Agency Rules), because this system is exempt from the access provisions of 5 U.S.C. 552a(d).

(H) From subsection (e)(5) because many of the records in this system coming from other system of records are derived from other agency record systems and therefore it is not possible for NGA to ensure their compliance with this provision, however, NGA has implemented internal quality assurance procedures to ensure that data used in the matching process is as thorough, accurate, and current as possible. In addition, in the collection of information for law enforcement, counterterrorism, and intelligence purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by (e)(5) would limit the ability of those agencies' trained investigators and intelligence analysts to exercise their judgment in conducting investigations and impede the development of intelligence necessary for effective law enforcement and counterterrorism efforts. However, NGA has implemented internal quality assurance procedures to ensure that the data used in the matching process is as thorough, accurate, and current as possible.

(I) From subsection (e)(8) because to require individual notice of disclosure of information due to compulsory legal process would pose an impossible administrative burden on NGA and other agencies and could alert the subjects of counterterrorism, law enforcement, or intelligence investigations to the fact of those investigations when not previously known.

(J) From subsection (f) (Agency Rules) because portions of this system are exempt from the access and amendment provisions of subsection (d).

(K) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act.

(d) *System identifier and name:* NGA–003, National Geospatial-Intelligence Agency Enterprise Workforce System.

(1) Exemptions: Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identity of a confidential source.

NOTE TO PARAGRAPH (d)(1): When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

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

(3) Reasons: Pursuant to 5 U.S.C. 552a (k)(2), the Director of NGA has exempted this system from the following provisions of the Privacy Act, subject to the limitation set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(i) From subsection (c)(3) and (c)(4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of NGA as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or

evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(ii) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of NGA or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(iii) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(iv) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(v) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(vi) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore NGA is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(vii) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude NGA personnel from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(viii) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with NGA's ability to cooperate with law enforcement who would obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(ix) From subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

(e) *System identifier and name:* NGA–008, National Geospatial-Intelligence Agency Polygraph Records System.

(1) Exemptions: Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access

to the information exempt to the extent that disclosure would reveal the identity of a confidential source.

NOTE TO PARAGRAPH (e)(1): When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

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

(3) Reasons: Pursuant to 5 U.S.C. 552a (k)(2), the Director of NGA has exempted this system from the following provisions of the Privacy Act, subject to the limitation set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(i) From subsection (c)(3) and (c)(4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of NGA as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(ii) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of NGA or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(iii) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(iv) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(v) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(vi) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore NGA is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(vii) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information

is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude NGA personnel from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(viii) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with NGA's ability to cooperate with law enforcement who would obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(ix) From subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

(f) *System identifier and name:* NGA–010, National Geospatial-Intelligence Agency Security Financial Disclosure Reporting Records System.

(1) Exemptions: Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identity of a confidential source. When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions. Investigative material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

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

(3) Reasons: Pursuant to 5 U.S.C. 552a(k)(2), and (k)(5) the Director of NGA has exempted this system from the following provisions of the Privacy Act, subject to the limitation set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(i) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of NGA as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process. Analyst case notes will be kept separate from the individual's data submission. Those case notes will contain investigative case leads and summaries, sensitive processes, evidence gathered from external sources and potential referrals to law enforcement agencies.

(ii) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of NGA or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(iii) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(iv) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore NGA is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

[66 FR 52681, Oct. 17, 2001, as amended at 67 FR 55724, Aug. 30, 2002; 78 FR 32555, May 31, 2013; 78 FR 69290, 69292, Nov. 19, 2013; 79 FR 26121, May 7, 2014; 80 FR 25231, May 4, 2015]

PART 321—DEFENSE SECURITY SERVICE PRIVACY PROGRAM

Sec.

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

SOURCE: 64 FR 49660, Sept. 14, 1999, unless otherwise noted.

§ 321.1 Purpose and applicability.

(a) This part establishes rules, policies and procedures for the disclosure of personal records in the custody of the Defense Security Service (DSS) to the individual subjects, the handling of requests for amendment or correction of such records, appeal and review of DSS decisions on these matters, and the application of general and specific exemptions, under the provisions of the Privacy Act of 1974. It also prescribes other policies and procedures to effect compliance with the Privacy Act of 1974 and DoD Directive 5400.11[1].

(b) The procedures set forth in this part do not apply to DSS personnel seeking access to records pertaining to themselves which previously have been available. DSS personnel will continue to be granted ready access to their personnel, security, and other records by making arrangements directly with the maintaining office. DSS personnel should contact the Office of Freedom of Information and Privacy, DSSHQ, for access to investigatory records pertaining to themselves or any assistance in obtaining access to other records pertaining to themselves, and may follow the procedures outlined in these rules in any case.

§ 321.2 Definitions.

(a) All terms used in this part which are defined in 5 U.S.C. 552a shall have the same meaning herein.

(b) As used in this part, the term agency means the Defense Security Service.

§ 321.3 Information and procedures for requesting notification.

(a) *General.* Any individual may request and receive notification of whether he is the subject of a record in any system of records maintained by DSS using the information and procedures described in this section.

(1) Paragraphs (b) and (c) of this section give information that will assist an individual in determining in what systems of DSS records (if any) he may

[1] Copies may be obtained via internet at *http://web7.whs.osd.mil/corres.htm.*

be the subject. This information is presented as a convenience to the individual in that he may avoid consulting the lengthy systems notices elsewhere in the FEDERAL REGISTER.

(2) Paragraph (d) of this section details the procedure an individual should use to contact DSS and request notification. It will be helpful if the individual states what his connection with DSS has or may have been, and about what record system(s) he is inquiring. Such information is not required, but its absence may cause some delay.

(b) *DSS Records Systems.* A list of DSS records systems is available by contacting Defense Security Service, Office of FOI and Privacy, 1340 Braddock Place, Alexandria, VA, 22314-1551.

(c) *Categories of individuals in DSS Record Systems.* (1) Any person who is the subject or co-subject of an ongoing or completed investigation by DSS should have an investigative case file/record in system V5-01, if the record meets retention criteria. An index to such files should be in V5-02.

(2) If an individual has ever made a formal request to DSS under the Freedom of Information Act or the Privacy Act of 1974, a record pertaining to that request under the name of the requester, or subject matter, will be in system V1-01.

(3) Persons of Counterintelligence interest who have solicited from industrial contractors/DoD installations information which may appear to be sensitive in nature may have a record in system V5-04.

(4) Individuals who have been applicants for employment with DSS, or nominees for assignment to DSS, but who have not completed their DSS affiliation, may be subjects in systems V4-04, V5-01, V5-02, V5-03, or V6-01.

(5) Any individual who is a subject, victim or cross-referenced personally in an investigation by an investigative element of any DoD component, may be referenced in the Defense Clearance and Investigations Index, system V5-02, in an index to the location, file number, and custodian of the case record.

(6) Individuals who have ever presented a complaint to or have been connected with a DSS Inspector General inquiry may be subjects of records in system V2-01.

(7) If an individual has ever attended the Defense Industrial Security Institute or completed training with the DSS Training Office he should be subject of a record in V7-01.

(8) If an individual has ever been a guest speaker or instructor at the Defense Industrial Security Institute, he should be the subject of a record in V7-01.

(9) If an individual is an employee or major stockholder of a government contractor or other DoD-affiliated company or agency and has been issued, now possesses or has been processed for a security clearance, he may be subject to a record in V5-03.

(d) *Procedures.* The following procedures should be followed to determine if an individual is a subject of records maintained by DSS, and to request notification and access.

(1) Individuals should submit inquiries in person or by mail to the Defense Security Service, Office of FOI and Privacy, 1340 Braddock Place, Alexandria, VA 22314-1651. Inquiries by personal appearance should be made Monday through Friday from 8:30 to 11:30 a.m. and 1:00 to 4:00 p.m. The information requested in Sec. 321.4 must be provided if records are to be accurately identified. Telephonic requests for records will not be honored. In a case where the system of records is not specified in the request, only systems that would reasonably contain records of the individual will be checked, as described in paragraph (b) of this section.

(2) Only the Director or Chief, Office of FOI and Privacy may authorize exemptions to notification of individuals in accordance with § 321.13.

§ 321.4 Requirements for identification.

(a) *General.* Only upon proper identification, made in accordance with the provisions of this section, will any individual be granted notification concerning and access to all releasable records pertaining to him which are maintained in a DSS system.

(b) *Identification.* Identification of individuals is required both for accurate record identification and to verify identity in order to avoid disclosing

records to unauthorized persons. Individuals who request notification of, access to, or amendment of records pertaining to themselves, must provide their full name (and additional names such as aliases, maiden names, alternate spellings, etc., if a check of these variants is desired), date and place of birth, and social security number (SSN).

(1) Where reply by mail is requested, a mailing address is required, and a telephone number is recommended to expedite certain matters. For military requesters residing in the United States, home address or P.O. Box number is preferred in lieu of duty assignment address.

(2) Signatures must be notarized on requests received by mail. Exceptions may be made when the requester is well known to releasing officials. For requests made in person, a photo identification card, such as military ID, driver's license or building pass, must be presented.

(3) While it is not required as a condition of receiving notification, in many cases the SSN may be necessary to obtain an accurate search of DCII (V5-02) records.

(c) A DSS Form 30 (Request for Notification of/Access to Personal Records) will be provided to any individual inquiring about records pertaining to himself whose mailed request was not notarized. This form is also available at the DSS Office of FOI and Privacy, 1340 Braddock Place, Alexandria, VA 22314-1651, for those who make their requests in person.

§ 321.5 Access by subject individuals.

(a) *General.* (1) Individuals may request access to records pertaining to themselves in person or by mail in accordance with this section. However, nothing in this section shall allow an individual access to any information compiled or maintained by DSS in reasonable anticipation of a civil or criminal action or proceeding, or otherwise exempted under the provisions of § 321.13.

(2) A request for a pending personnel security investigation will be held in abeyance until completion of the investigation and the requester will be so notified.

(b) *Manner of access.* (1) Requests by mail or in person for access to DSS records should be made to the DSS Office of FOI and Privacy, 1340 Braddock Place, Alexandria, VA 22314-1651.

(2) Any individual who makes a request for access in person shall:

(i) Provide identification as specified in Sec. 321.4.

(ii) Complete and sign a request form.

(3) Any individual making a request for access to records by mail shall include a signed and notarized statement to verify his identity, which may be the DSS request form if he has received one.

(4) Any individual requesting access to records in person may be accompanied by an identified person of his own choosing while reviewing the record. If the individual elects to be accompanied, he shall make this known in his written request, and include a statement authorizing disclosure of the record contents to the accompanying person. Without written authorization of the subject individual, records will not be disclosed to third parties accompanying the subject.

(5) During the course of official business, members of DSS field elements may be given access to records maintained by the field elements/Operations Center without referral to the Office of FOI and Privacy. An account of such access will be kept for reporting purposes.

(6) In all requests for access, the requester must state whether he or she desires access in person or mailed copies of records. During personal access, where copies are made for retention, a fee for reproduction and postage may be assessed as provided in Sec. 321.11. Where copies are mailed because personal appearance is impractical, there will be no fee.

(7) All individuals who are not affiliates of DSS will be given access to records, if authorized, in the Office of FOI and Privacy, or by means of mailed copies.

§ 321.6 Medical records.

General. Medical records that are part of DSS records systems will generally be included with those records when access is granted to the subject to which they pertain. However, if it is

determined that such access could have an adverse effect upon the individual's physical or mental health, the medical record in question will be released only to a physician named by the requesting individual.

§ 321.7 Request for correction or amendment.

(a) *General.* Upon request and proper identification by any individual who has been granted access to DSS records pertaining to himself or herself, that individual may request, either in person or through the mail, that the record be amended. Such a request must be made in writing and addressed to the Defense Security Service, Office of FOI and Privacy, 1340 Braddock Place, Alexandria, VA 22314-1651.

(b) *Content.* The following information must be included to insure effective action on the request:

(1) Description of the record. Requesters should specify the number of pages and documents, the titles of the documents, form numbers if there are any, dates on the documents and names of individuals who signed them. Any reasonable description of the document is acceptable.

(2) Description of the items to be amended. The description of the passages, pages or documents to be amended should be as clear and specific as possible.

(i) Page, line and paragraph numbers should be cited where they exist.

(ii) A direct quotation of all or a portion of the passage may be made if it isn't otherwise easily identifiable. If the passage is long, a quotation of its beginning and end will suffice.

(iii) In appropriate cases, a simple substantive request may be appropriate, e.g., 'delete all references to my alleged arrest in July 1970.'

(iv) If the requester has received a copy of the record, he may submit an annotated copy of documents he wishes amended.

(3) Type of amendment. The requester must clearly state the type of amendment he is requesting.

(i) Deletion or expungement, i.e., a complete removal from the record of data, sentences, passages, paragraphs or documents.

(ii) Correction of the information in the record to make it more accurate, e.g., rectify mistaken identities, dates, data pertaining to the individual, etc.

(iii) Additions to make the record more relevant, accurate or timely may be requested.

(iv) Other changes may be requested; they must be specifically and clearly described.

(4) Reason for amendment. Requests for amendment must be based on specific reasons, included in writing. Categories of reasons are as follows:

(i) Accuracy. Amendment may be requested where matters of fact are believed incorrectly recorded, e.g., dates, names, addresses, identification numbers, or any other information concerning the individual. The request, whenever possible, should contain the accurate information, copies of verifying documents, or indication of how the information can be verified.

(ii) Relevance. Amendment may be requested when information in a record is believed not to be relevant or necessary to the purposes of the record system.

(iii) Timeliness. Amendment may be requested when information is thought to be so old as to no longer be pertinent to the stated purposes of the records system. It may also be requested when there is recent information of a pertinent type that is not included in the record.

(iv) Completeness. Amendment may be requested where information in a record is incomplete with respect to its purpose. The data thought to have been omitted should be included or identified with the request.

(v) Fairness. Amendment may be requested when a record is thought to be unfair concerning the subject, in terms of the stated purposes of the record. In such cases, a source of additional information to increase the fairness of the record should be identified where possible.

(vi) Other reasons. Reasons for requesting amendment are not limited to those cited above. The content of the records is authorized in terms of their stated purposes which should be the basis for evaluating them. However, any matter believed appropriate may

be submitted as a basis of an amendment request.

(vii) Court orders and statutes may require amendment of a file. While they do not require a Privacy Act request for execution, such may be brought to the attention of DSS by these procedures.

(c) *Assistance.* Individuals seeking to request amendment of records pertaining to themselves that are maintained by DSS will be assisted as necessary by DSS officials. Where a request is incomplete, it will not be denied, but the requester will be contacted for the additional information necessary to his request.

(d) This section does not permit the alteration of evidence presented to courts, boards and other official proceedings.

§ 321.8 DSS review of request for amendment.

(a) *General.* Upon receipt from any individual of a request to amend a record pertaining to himself and maintained by the Defense Security Service, Office of FOI and Privacy will handle the request as follows:

(1) A written acknowledgment of the receipt of a request for amendment of a record will be provided to the individual within 10 working days, unless final action regarding approval or denial can be accomplished within that time. In that case, the notification of approval or denial will constitute adequate acknowledgment.

(2) Where there is a determination to grant all or a portion of a request to amend a record, the record shall be promptly amended and the requesting individual notified. Individuals, agencies or components shown by accounting records to have received copies of the record, or to whom disclosure has been made, will be notified, if necessary, of the amendment by the responsible official. Where a DoD recipient of an investigative record cannot be located, the notification, if necessary, will be sent to the personnel security element of the parent Component.

(3) Where there is a determination to deny all or a portion of a request to amend a record, the office will promptly:

(i) Advise the requesting individual of the specifics of the refusal and the reasons;

(ii) Inform the individual that he may request a review of the denial(s) from 'Director, Defense Security Service, 1340 Braddock Place, Alexandria, VA 22314-1651.' The request should be brief, in writing, and enclose a copy of the denial correspondence.

(b) DSS determination to approve or deny. Determination to approve or deny and request to amend a record or portion thereof may necessitate additional investigation or inquiry be made to verify assertions of individuals requesting amendment. Coordination will be made with the Director for Investigations and the Director of the Personnel Investigations Center in such instances.

§ 321.9 Appeal of initial amendment decision.

(a) *General.* Upon receipt from any individual of an appeal to review a DSS refusal to amend a record, the Defense Security Service, Office of FOI and Privacy will assure that such appeal is handled in compliance with the Privacy Act of 1974 and DoD Directive 5400.11 and accomplish the following:

(1) Review the record, request for amendment, DSS action on the request and the denial, and direct such additional inquiry or investigation as is deemed necessary to make a fair and equitable determination.

(2) Recommend to the Director whether to approve or deny the appeal.

(3) If the determination is made to amend a record, advise the individual and previous recipients (or an appropriate office) where an accounting of disclosures has been made.

(4) Where the decision has been made to deny the individual's appeal to amend a record, notify the individual:

(i) Of the denial and the reason;

(ii) Of his right to file a concise statement of reasons for disagreeing with the decision not to amend the record;

(iii) That such statement may be sent to the Defense Security Service, Office of FOI and Privacy, (GCF), 1340 Braddock Place, Alexandria, VA 22314-1651, and that it will be disclosed to users of the disputed record;

(iv) That prior recipients of the disputed record will be provided a copy of the statement of disagreement, or if they cannot be reached (e.g., through deactivation) the personnel security element of their DoD component;

(v) And, that he may file a suit in a Federal District Court to contest DSS's decision not to amend the disputed record.

(b) *Time limit for review of appeal.* If the review of an appeal of a refusal to amend a record cannot be accomplished within 30 days, the Office of FOI and Privacy will notify the individual and advise him of the reasons, and inform him of when he may expect the review to be completed.

§ 321.10 Disclosure to other than subject.

(a) *General.* No record contained in a system of records maintained by DSS shall be disclosed by any means to any person or agency outside the Department of Defense, except with the written consent or request of the individual subject of the record, except as provided in this section. Disclosures that may be made without the request or consent of the subject of the record are as follows:

(1) To those officials and employees of the Department of Defense who have a need for the record in the performance of their duties, when the use is compatible with the stated purposes for which the record is maintained.

(2) Required to be disclosed by the Freedom of Information Act.

(3) For a routine use as described in DoD Directive 5400.11.

(4) To the Census Bureau, National Archives, the U.S. Congress, the Comptroller General or General Accounting Office under the conditions specified in DoD Directive 5400.11.

(5) At the written request of the head of an agency outside DoD for a law enforcement activity as authorized by DoD Directive 5400.11.

(6) For statistical purposes, in response to a court order, or for compelling circumstances affecting the health or safety of an individual as described in DoD Directive 5400.11.

(7) Legal guardians recognized by the Act.

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

(1) Accounting entries will normally be kept on a DSS 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) An accounting of disclosures made to agencies outside the DoD of records in the Defense Clearance and Investigations Index (V5-02) will be kept as prescribed by the Director of Systems, DSS.

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

(5) Subjects of DSS records will be given access to associated accounting records upon request, except as exempted under § 321.13.

§ 321.11 Fees.

Individuals may request copies for retention of any documents to which they are granted access in DSS records pertaining to them. Requestors 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 DoD Directive 5400.11.

§ 321.12 Penalties.

(a) An individual may bring a civil action against the DSS to correct or amend the record, or where there is a refusal to comply with an individual request or failure to maintain any record with accuracy, relevance, timeliness and completeness, so as to guarantee fairness, or failure to comply with any other provision of 5 U.S.C. 552a. The court may order correction or amendment. It may assess against the United States reasonable attorney fees and other costs, or may enjoin the DSS

from withholding the records and order the production to the complainant.

(b) Where it is determined that the action was willful or intentional with respect to 5 U.S.C. 552a(g)(1) (C) or (D), the United States shall be liable for the actual damages sustained, but in no case less than the sum of $1,000 and the costs of the action with attorney fees.

(c) Criminal penalties may be imposed against an officer or employee of the DSS who fully discloses material, which he knows is prohibited from disclosure, or who willfully maintains a system of records without the notice requirements; or against any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses. These offenses shall be misdemeanors with a fine not to exceed $5,000.

§ 321.13 Exemptions.

(a) *General.* The Director of the Defense Security Service establishes the following exemptions of records systems (or portions thereof) from the provisions of these rules, and other indicated portions of Pub. L. 93-579, in this section. They may be exercised only by the Director, Defense Security Service and the Chief of the Office of FOI and Privacy. Exemptions will be exercised only when necessary for a specific, significant and legitimate reason connected with the purpose of a records system, and not simply because they are authorized by statute. Personal records releasable under the provisions of 5 U.S.C. 552 will not be withheld from subject individuals based on these exemptions.

(b) All systems of records maintained by DSS shall be exempt from the requirements of 5 U.S.C. 552a(d) pursuant to 5 U.S.C. 552a(k)(1) to the extent that the system contains any information properly classified under Executive Order 12958 and which is required by the Executive Order to be withheld in the interest of national defense of 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 herein may contain items of information that have been properly classified.

(c) *System identifier:* V1-01.

(1) System name: Privacy and Freedom of Information Request Records.

(2) Exemptions: (i) Investigatory material compiled for law enforcement purposes may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source.

(ii) Records maintained in connection with providing protective services to the President and other individuals under 18 U.S.C. 3506, may be exempt pursuant to 5 U.S.C. 552a(k)(3).

(iii) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(iv) Any portion of this system that falls under the provisions of 5 U.S.C. 552a(k)(2), (k)(3), (k)(5) may be exempt from the following subsections of 5 U.S.C. 552a(c)(3); (d); (e)(1); (e)(4)(G), (H) and (I); and (f).

(3) Authority: 5 U.S.C. 552a(k)(2), (k)(3), (k)(5).

(4) Reasons: (i) From subsection (c)(3) because it will enable DSS 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 subsections (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);

(iii) From subsections (d) and (f) because requiring DSS to grant access to records and agency rules for access and amendment of records would unfairly impede the agency's investigation of allegations of unlawful activities. To require DSS to confirm or deny the existence of a record pertaining to a requesting individual may in itself provide an answer to that individual relating to an on-going investigation. The investigation of possible unlawful activities would be jeopardized by agency rules requiring verification of record, disclosure of the record to the subject, and record amendment procedures.

(d) *System identifier:* V5-01.

(1) System name: Investigative Files System

(2) Exemption: (i) Investigatory material compiled for law enforcement purposes may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source.

(ii) Records maintained in connection with providing protective services to the President and other individuals under 18 U.S.C. 3506, may be exempt pursuant to 5 U.S.C. 552a(k)(3).

(iii) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(iv) Any portion of this system that falls under the provisions of 5 U.S.C. 552a(k)(2), (k)(3), or (k)(5) may be exempt from the following subsections of 5 U.S.C. 552a(c)(3); (d); (e)(1); (e)(4)(G), (H), and (I); and (f).

(3) Authority: 5 U.S.C. 552a(k)(2), (k)(3), or (k)(5).

(4) Reasons: (i) From subsection (c)(3) because it will enable DSS 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 subsections (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).

(iii) From subsections (d) and (f) because requiring DSS to grant access to records and agency rules for access and amendment of records would unfairly impede the agency's investigation of allegations of unlawful activities. To require DSS to confirm or deny the existence of a record pertaining to a requesting individual may in itself provide an answer to that individual relating to an on-going investigation. The investigation of possible unlawful activities would be jeopardized by agency rules requiring verification of record, disclosure of the record to the subject, and record amendment procedures.

(e) *System identifier:* V5-02.

(1) System name: Defense Clearance and Investigations Index (DCII).

(2) Exemption: Investigatory material compiled for law enforcement purposes may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source. Any portion of this system that falls under the provisions of 5 U.S.C. 552a(k)(2) may be exempt from the following subsections of 5 U.S.C. 552a(c)(3); (d); (e)(1); (e)(4)(G), (H), and (I), and (f).

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

(4) Reasons: (i) From subsection (c)(3) because it will enable DSS 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 subsections (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).

(iii) From subsections (d) and (f) because requiring DSS to grant access to records and agency rules for access and amendment of records would unfairly impede the agency's investigation of allegations of unlawful activities. To require DSS to confirm or deny the existence of a record pertaining to a requesting individual may in itself provide an answer to that individual relating to an on-going investigation. The investigation of possible unlawful activities would be jeopardized by agency rules requiring verification of record, disclosure of the record to the subject, and record amendment procedures.

(f) *System identifier:* V5-03.

(1) System name: Case Control Management System (CCMS).

(2) Exemption: (i) Investigatory material compiled for law enforcement purposes may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source.

(ii) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source. Any portion of this system that falls under the provisions of 5 U.S.C. 552a(k)(2) or (k)(5) may be exempt from the following subsections of 5 U.S.C. 552a: (c)(3); (d); (e)(1); (e)(4)(G), (H), and (I); and (f).

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

(4) Reasons. (i) From subsection (c)(3) because it will enable DSS 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 subsections (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).

(iii) From subsections (d) and (f) because requiring DSS to grant access to records and agency rules for access and amendment of records would unfairly impede the agency's investigation of allegations of unlawful activities. To require DSS to confirm or deny the existence of a record pertaining to a requesting individual may in itself provide an answer to that individual relating to an on-going investigation. The investigation of possible unlawful activities would be jeopardized by agency rules requiring verification of record, disclosure of the record to the subject, and record amendment procedures.

(g) *System identifier:* V5-04.

(1) System name: Counterintelligence Issues Database (CII-DB).

(2) Exemption: (i) Information specifically authorized to be classified under E.O. 12958, as implemented by DoD 5200.1-R, may be exempt pursuant to 5 U.S.C. 552a(k)(1).

(ii) Investigatory material compiled for law enforcement purposes may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source.

(iii) Records maintained in connection with providing protective services to the President and other individuals under 18 U.S.C. 3506, may be exempt pursuant to 5 U.S.C. 552a(k)(3).

(iv) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(v) Any portion of this system that falls within the provisions of 5 U.S.C. 552a(k)(1), (k)(2), (k)(3) and (k)(5) may be exempt from the following subsections (c)(3); (d)(1) through (d)(5); (e)(1); (e)(4)(G), (H), and (I); and (f).

(3) Authority. 5 U.S.C. 552a(k)(1), (k)(2), (k)(3) and (k)(5).

(4) Reasons. (i) From subsection (c)(3) because giving the individual access to the disclosure accounting could alert the subject of an investigation to the existence and nature of the investigation and reveal investigative or prosecutive interest by other agencies, particularly in a joint-investigation situation. This would seriously impede or compromise the investigation and case preparation by prematurely revealing its existence and nature; compromise or interfere with witnesses or make witnesses reluctant to cooperate with the investigators; lead to suppression, alteration, fabrication, or destruction of evidence; and endanger the physical safety of confidential sources, witnesses, law enforcement personnel and their families.

(ii) From subsection (d) because the application of these provisions could impede or compromise an investigation or prosecution if the subject of an investigation had access to the records or were able to use such rules to learn of the existence of an investigation before it would be completed. In addition, the mere notice of the fact of an investigation could inform the subject and others that their activities are under or may become the subject of an investigation and could enable the subjects to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

(iii) From subsection (e)(1) because during an investigation it is not always possible to detect the relevance or necessity of each piece of information in

the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear. In other cases, what may appear to be a relevant and necessary piece of information may become irrelevant in light of further investigation. In addition, during the course of an investigation, the investigator may obtain information that related primarily to matters under the investigative jurisdiction of another agency, and that information may not be reasonably segregated. In the interest of effective law enforcement, DSS investigators should retain this information, since it can aid in establishing patterns of criminal activity and can provide valuable leads for Federal and other law enforcement agencies.

(iv) From subsections (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f) because this system is exempt from subsection (d) of the Act, concerning access to records. These requirements are inapplicable to the extent that these records will be exempt from these subsections. However, DSS has published information concerning its notification and access procedures, and the records source categories because under certain circumstances, DSS could decide it is appropriate for an individual to have access to all or a portion of his/her records in this system of records.

(h) [Reserved]

[64 FR 49660, Sept. 14, 1999, as amended at 70 FR 38009, July 1, 2005; 76 FR 22808, Apr. 25, 2011]

§ 321.14 DSS implementation policies.

(a) *General.* The implementation of the Privacy Act of 1974 within DSS is as prescribed by DoD Directive 5400.11. This section provides special rules and information that extend or amplify DoD policies with respect to matters of particular concern to the Defense Security Service.

(b) *Privacy Act rules application.* Any request which cites neither Act, concerning personal record information in a system or records, by the individual to whom such information pertains, for access, amendment, correction, accounting of disclosures, etc., will be governed by the Privacy Act of 1974, DoD Directive 5400.11 and these rules exclusively. Requests for like information which cite only the Freedom of Information Act will be governed by the Freedom of Information Act, DoD Regulation 5400.7R[2]. Any denial or exemption of all or part of a record from notification, access, disclosure, amendment or other provision, will also be processed under these rules, unless court order or other competent authority directs otherwise.

(c) *First amendment rights.* No DSS official or element may maintain any information pertaining to the exercise by an individual of his rights under the First Amendment without the permission of that individual unless such collection is specifically authorized by statute or necessary to and within the scope of an authorized law enforcement activity.

(d) *Standards of accuracy and validation of records.* (1) All individuals or elements within DSS which create or maintain records pertaining to individuals will insure that they are reasonably accurate, relevant, timely and complete to serve the purpose for which they are maintained and to assure fairness to the individual to whom they pertain. Information that is not pertinent to a stated purpose of a system of records will not be maintained within those records. Officials compiling investigatory records will make every reasonable effort to assure that only reports that are impartial, clear, accurate, complete, fair and relevant with respect to the authorized purpose of such records are included, and that reports not meeting these standards or serving such purposes are not included in such records.

(2) Prior to dissemination to an individual or agency outside DoD of any record about an individual (except for a Freedom of Information Act action or access by a subject individual under these rules) the disclosing DSS official will by review, make a reasonable effort to assure that such record is accurate, complete, timely, fair and relevant to the purpose for which they are maintained.

(e) *The Defense Clearance and Investigations Index (DCII).* It is the policy of

[2] See footnote 1 to 321.1.

DSS, as custodian, that each DoD component or element that has direct access to or contributes records to the DCII (V5-02), is individually responsible for compliance with the Privacy Act of 1974 and DoD Directive 5400.11 with respect to requests for notification, requests for access by subject individuals, granting of such access, request for amendment and corrections by subjects, making amendments or corrections, other disclosures, accounting for disclosures and the exercise of exemptions, insofar as they pertain to any record placed in the DCII by that component or element. Any component or element of the DoD that makes a disclosure of any record whatsoever to an individual or agency outside the DoD, from the DCII, is individually responsible to maintain an accounting of that disclosure as prescribed by the Privacy Act of 1974 and DoD Directive 5400.11 and to notify the element placing the record in the DCII of the disclosure. Use of and compliance with the procedures of the DCII Disclosure Accounting System will meet these requirements. Any component or element of DoD with access to the DCII that, in response to a request concerning an individual, discovers a record pertaining to that individual placed in the DCII by another component or element, may refer the requester to the DoD component that placed the record into the DCII without making an accounting of such referral, although it involves the divulging of the existence of that record. Generally, consultation with, and referral to, the component or element placing a record in the DCII should be effected by any component receiving a request pertaining to that record to insure appropriate exercise of amendment or exemption procedures.

(f) *Investigative operations.* (1) DSS agents must be thoroughly familiar with and understand these rules and the authorities, purposes and routine uses of DSS investigative records, and be prepared to explain them and the effect of refusing information to all sources of investigative information, including subjects, during interview, in response to questions that go beyond the required printed and oral notices. Agents shall be guided by DSS Handbook for Personnel Security Investigations in this respect.

(2) All sources may be advised that the subject of an investigative record may be given access to it, but that the identities of sources may be withheld under certain conditions. Such advisement will be made as prescribed in DSS Handbook for Personnel Security Investigations, and the interviewing agent may not urge a source to request a grant of confidentiality. Such pledges of confidence will be given sparingly and then only when required to obtain information relevant and necessary to the stated purpose of the investigative information being collected.

(g) *Non-system information on individuals.* The following information is not considered part of personal records systems reportable under the Privacy Act of 1974 and may be maintained by DSS members for ready identification, contact, and property control purposes only. If at any time the information described in this paragraph is to be used for other than these purposes, that information must become part of a reported, authorized record system. No other information concerning individuals except that described in the records systems notice and this paragraph may be maintained within DSS.

(1) Identification information at doorways, building directories, desks, lockers, name tags, etc.

(2) Identification in telephone directories, locator cards and rosters.

(3) Geographical or agency contact cards.

(4) Property receipts and control logs for building passes, credentials, vehicles, weapons, etc.

(5) Temporary personal working notes kept solely by and at the initiative of individual members of DSS to facilitate their duties.

(h) *Notification of prior recipients.* Whenever a decision is made to amend a record, or a statement contesting a DSS decision not to amend a record is received from the subject individual, prior recipients of the record identified in disclosure accountings will be notified to the extent possible. In some cases, prior recipients cannot be located due to reorganization or deactivations. In these cases, the personnel

security element of the receiving Defense Component will be sent the notification or statement for appropriate action.

(i) *Ownership of DSS Investigative Records.* Personnel security investigative reports shall not be retained by DoD recipient organizations. Such reports are considered to be the property of the investigating organization and are on loan to the recipient organization for the purpose for which requested. All copies of such reports shall be destroyed within 120 days after the completion of the final personnel security determination and the completion of all personnel action necessary to implement the determination. Reports that are required for longer periods may be retained only with the specific written approval of the investigative organization.

(j) *Consultation and referral.* DSS system of records may contain records originated by other components or agencies which may have claimed exemptions for them under the Privacy Act of 1974. When any action that may be exempted is initiated concerning such a record, consultation with the originating agency or component will be effected. Where appropriate such records will be referred to the originating component or agency for approval or disapproval of the action.

PART 322—NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICES PRIVACY ACT PROGRAM

Sec.
322.1 Purpose and applicability.
322.2 Definitions.
322.3 Policy.
322.4 Responsibilities.
322.5 Procedures.
322.6 Establishing exemptions.
322.7 Exempt systems of records.

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

SOURCE: 68 FR 28757, May 27, 2003, unless otherwise noted.

§ 322.1 Purpose and applicability.

(a) This part implements the Privacy Act of 1974 (5 U.S.C. 552a), as amended and the Department of Defense Privacy Program (32 CFR part 310) within the National Security Agency/Central Security Service (NSA/CSS); establishes policy for the collection and disclosure of personal information about individuals; assigns responsibilities and establishes procedures for collecting personal information and responding to first party requests for access to records, amendments of those records, or an accounting of disclosures.

(b) This part applies to all NSA/CSS elements, field activities and personnel and governs the release or denial of any information under the terms of the Privacy Act of 1974 (5 U.S.C. 552a), as amended.

§ 322.2 Definitions.

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

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.

Employees of NSA/CSS. Individuals employed by, assigned or detailed to the NSA/CSS. This part also applies to NSA/CSS contractor personnel who administer NSA/CSS systems of records that are subject to the Privacy Act.

FOIA Request. A written request for NSA/CSS records, made by any person, that either explicitly or implicitly invokes the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended. FOIA requests will be accepted by U.S. mail or its equivalent, facsimile, or the Internet, or employees of NSA/CSS may hand deliver them.

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.

Maintain. Includes maintain, collect, use or disseminate.

Medical Records. Documents relating to the physical care and treatment of an individual.

Privacy Act Request. A written request containing a signature submitted by a U.S. citizen or alien admitted for permanent residence for access to or amendment of records on himself/herself which are contained in a PA system of records. PA requests will be accepted via mail or facsimile, or NSA/CSS employees may hand deliver them. Digital signatures will be accepted via the Internet by October 21, 2003. Until then, PA requests will not be accepted via the Internet. Requests received via the Internet will not be acknowledged. Regardless of whether the requester cites the FOIA, PA, or no law, the request for records will be processed under both this part and the FOIA. Requests for amendments will be processed pursuant to the PA.

Personal information. The collection of two or more pieces of information that is about an individual: e.g., name and date of birth, Social Security Number.

Personal notes. Notations created in paper or electronic form for the convenience and at the discretion of the originator, for the originator's eyes only, and over which NSA/CSS exercises no control. Personal notes are not agency records within the meaning of the Privacy Act (PA) or the Freedom of Information Act (FOIA). However, once the personal note, or information contained therein, is shared with another individual, it becomes an Agency record and is subject to the provisions of the FOIA and, if appropriate, the PA.

Psychological Records. Documents relating to the psychological care and treatment of an individual.

Record. Any item, collection, or grouping of information, whatever the storage media (paper, electronic, etc.) about an individual or 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 fingerprint, voice print, or a photograph. The record must be in existence and under the control of NSA/CSS at the time a request is made.

Routine use. The disclosure of a record outside NSA/CSS or the DoD for a use that is compatible with the purpose for which the information was collected and maintained by NSA/CSS. The routine use must be included in the published system of records.

System of Records. A group of records under the control of a federal agency 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

§ 322.3 Policy.

(a) The National Security Agency/Central Security Service shall maintain in its records only such information about an individual that is relevant and necessary to accomplish a purpose of the Agency, and that is required or authorized to be maintained by statute or Executive Order. Information about an individual shall, to the greatest extent practicable, be collected directly from the individual if the information may result in adverse determinations about the individual's rights, benefits, and privileges under any Federal program. Records used by this Agency in making adverse determinations about an individual shall be maintained with such accuracy, relevance, timeliness and completeness as is reasonably necessary to assure fairness to the individual. The Agency shall protect the privacy of individuals identified in its records, and shall permit an individual to request access to personal information in records on himself/herself and to request correction or amendment of factual information contained in such records. These policies are consistent with the spirit and intent of the PA, and are subject to exemptions under the Act, as defined in § 322.7, and legal requirements to protect sensitive NSA information such as the intelligence sources and

methods the Agency employs to fulfill its mission.

(b) Pursuant to written requests submitted in accordance with the PA, the NSA/CSS shall make records available consistent with the Act and the need to protect government interests pursuant to subsections (d) and (k) of the Privacy Act. Oral requests for information shall not be accepted. Before the Agency responds to a request, the request must comply with the provisions of this part.

(c) In order that members of the public have timely access to unclassified information regarding NSA activities, requests for information that would not be withheld if requested under the FOIA or the PA may be honored through appropriate means without requiring the requester to invoke the FOIA or the PA. Although a record may require minimal redaction before its release, this fact alone shall not require the Agency to direct the requester to submit a formal FOIA or PA request for the record.

§ 322.4 Responsibilities.

(a) The Director's Chief of Staff (DC) is responsible for overseeing the administration of the PA. The Director of Policy (DC3), or the Deputy Director of Policy, if so designated, shall carry out this responsibility on behalf of the Chief of Staff and shall:

(1) Provide policy guidance to NSA/CSS on PA issues.

(2) Provide policy guidance to PA coordinators for processing PA requests from NSA/CSS employees who will be using the records within NSA/CSS spaces.

(3) Provide training of NSA/CSS employees and contractors in the requirements of the PA. Specialized training is provided to special investigators and employees who deal with the news media or the public.

(4) Receive, process, and respond to PA requests from individuals and employees who require the information for use outside of NSA/CSS spaces.

(i) Conduct the appropriate search for and review of records.

(ii) Provide the requester with copies of all releasable material.

(iii) Notify the requester of any adverse determination, including his/her right to appeal an adverse determination to the NSA/CSS Appeal Authority.

(iv) Assure the timeliness of responses.

(5) Receive, process and respond to PA amendment requests to include:

(i) Obtain comments and supporting documentation from the organization originating the record.

(ii) Conduct a review of all documentation relevant to the request.

(iii) Advise the requester of the Agency's decision.

(iv) Notify the requester of any adverse determination, including his/her right to appeal the adverse determination to the NSA/CSS Appeal Authority.

(v) Direct the appropriate Agency organization to amend a record and advise other record holders to amend the record when a decision is made in favor of a requester.

(vi) Assure the timeliness of responses.

(6) Ensure that Agency employees (internal requesters) that have access to NSA/CSS spaces are given access to all or part of a PA record to which the employee was denied by the record holder when, after a review of the circumstances by the Director of Policy, it is determined that access should be granted. For those individuals who do not have access to NSA/CSS spaces see § 322.6 of this part.

(7) Conduct Agency reviews in accordance with OMB Circular A–130[1] and 32 CFR part 310.

(8) Deposit in the U.S. Treasury all fees collected as a result of charges levied for the duplication of records provided under the PA and maintain the necessary accounting records for such fees.

(b) The NSA/CSS Privacy Act Appeal Authority is designated as the reviewing authority for requests for review of denials by the Director of Policy to provide access to a record and/or to amend a record. The PA Appeal Authority is the Deputy Director, NSA. In the absence of the Deputy Director, the Director's Chief of Staff serves as the Appeal Authority.

(c) The General Counsel (GC) or his designee shall:

[1] Available from *http://www.whitehouse.gov/omb/circulars/index.html*.

(1) Advise on all legal matters concerning the PA.

(2) Advise the Director of Policy and other NSA/CSS organizations, as appropriate, of legal decisions including rulings by the Justice Department and actions by the DoD Privacy Board involving the PA.

(3) Review proposed responses to PA requests to ensure legal sufficiency, as appropriate.

(4) Provide a legal review of proposed Privacy Act notices and amendments for submission to the Defense Privacy Office.

(5) Assist, as required, in the preparation of PA reports for the Department of Defense and other authorities.

(6) Review proposals to collect PA information for legal sufficiency, assist in the development of PA statements and warning statements when required and approve prior to use.

(7) Represent the Agency in all judicial actions related to the PA by providing support to the Department of Justice and by keeping the DoD Office of General Counsel apprised of pending PA litigation. A litigation status sheet will be provided to the Defense Privacy Office.

(8) Assist in the education of new and current employees, including contractors, to the requirements of the PA.

(9) Review PA and PA Amendment appeals, prepare responses, and submit them to the NSA/CSS Appeal Authority for final decision.

(10) Notify the Director of Policy of the outcome of all appeals.

(d) The Associate Director for Human Resources Services or designee shall:

(1) Establish the physical security requirements for the protection of personal information and ensure that such requirements are maintained.

(2) Establish and ensure compliance with procedures governing the pledging of confidentiality to sources of information interviewed in connection with inquiries to determine suitability, eligibility or qualifications for Federal employment, Federal contracts, or access to classified information.

(3) Retain copies of records processed pursuant to the PA. The retention schedule is six years from the date records were provided to the requester if deletions were made and two years if records were provided in their entirety.

(4) Ensure the prompt delivery of all PA requests to the Director of Policy.

(5) Ensure the prompt delivery of all Privacy Act appeals of an adverse determination to the NSA/CSS PA Appeal Authority staff.

(6) Ensure that forms used to collect PA information meet the requirements of the PA.

(7) Compile, when required, estimates of cost incurred in the preparation or modification of forms requiring PA Statements.

(8) Assist in the development of training courses to educate new and current Agency employees, including contractors, of the provisions of the PA.

(9) Respond to PA requests for access to records, as appropriate.

(10) Establish procedures for the protection of personal information and ensure compliance with the procedures.

(e) The Inspector General (IG) shall:

(1) Be alert to Privacy Act compliance and to managerial administrative, and operational problems associated with the implementation of this part and document any such problems and remedial actions, if any, in official reports to responsible Agency officials, when appropriate.

(2) Respond, as appropriate, to PA requests.

(3) Establish procedures for the protection of personal records under the control or in the possession of OIG and ensure compliance with the procedures.

(f) Chiefs of Directorates, Associate Directorates, and Field Elements shall:

(1) Ensure that no systems or subsets of Systems of Records other than those published in the FEDERAL REGISTER are maintained within their components or field elements.

(2) Establish rules of conduct for persons who design, use or maintain Systems of Records within their components or field elements and ensure compliance with these rules.

(3) Establish, in consultation with the Associate Director of Human Resources or designee, the physical security requirements for the protection of personal information and ensure that such requirements are maintained.

(4) Ensure that no records are maintained within their components or field elements which describe how any individual exercises rights guaranteed by the First Amendment to the Constitution of the United States unless expressly authorized by statute, or by the individual about whom the record is maintained, or unless pertinent to, and within the scope of, an authorized law enforcement activity.

(5) Ensure that records contained in the Systems of Records within their components or field elements are not disclosed to anyone other than in conformance with the Privacy Act, to include the routine uses for such records published in the FEDERAL REGISTER.

(6) Maintain only such information about an individual as is relevant and necessary to accomplish a purpose of the Agency required to be accomplished by statute and Executive Order.

(7) Maintain all records which are used by the Agency in making any determination about any individual with such accuracy, relevancy, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual in any determination.

(8) Establish procedures for protecting the confidentiality of personal records maintained or processed by computer systems and ensure compliance with the procedures.

(9) Designate a primary and alternate PA coordinator to be responsible for PA matters and inform the Office of Policy of the designations. Subordinate PA coordinators may be appointed at office level.

(10) Ensure that the Privacy Act coordinators acquire the necessary training in the theory and administration of the Privacy Act.

(11) Ensure that the Privacy Act coordinators conduct, to the extent practicable, on-the-job PA training of supervisors and records handlers in their organizations.

(12) Respond to PA requests to review records, as appropriate.

(13) Establish procedures for the protection of personal records and ensure compliance with the procedures.

(14) Establish procedures to ensure that requests for copies of PA records needed for external use, outside of NSA/CSS, shall be delivered to the Director of Policy immediately upon receipt once the request is identified as a Privacy Act request or appears to be intended as such a request.

(15) Publish, as necessary, internal PA procedures which are consistent with the Privacy Act and this part.

(16) Maintain an accounting of disclosures of records as described in § 322.5 of this part.

(17) Coordinate with the Office of the General Counsel any proposed new record systems or changes (either alterations or amendments) to existing systems. Notice of new record systems or alterations to existing systems must be published in the FEDERAL REGISTER at least 30 days and Congress and the Office of Management and Budget must be given 40 days to review the new/altered system before implementation.

(18) Collect and forward to the Director of Policy information necessary to prepare reports, as requested.

(19) Respond promptly to the Director of Policy and the PA Appeal Authority decisions concerning the granting access to records, amending records, or filing statements of disagreements.

(20) Ensure that forms (paper or electronic) used to collect PA information meet the requirements of the PA.

(21) Establish procedures to ensure that requests to conduct computer matching are forwarded to the Director of Policy.

(g) Each field element shall designate a Privacy Act (PA) Coordinator to ensure compliance with this part and to receive and, where appropriate, process PA requests. Section 322.6 of this part describes the procedure for individuals to gain access to records and the responsibilities of the PA Coordinators. Consistent with the provisions of 32 CFR parts 285 and 286 and 32 CFR part 310 special procedures apply to the disclosure of certain medical records and psychological records. Field elements should consult the PA Coordinator of the Office of Occupational Health, Environment and Safety Services before disclosing such information. (*See* paragraph (d)(9) of this section.)

(h) All NSA/CSS organizations and field elements responsible for electronic/paper forms or other methods used to collect personal information

from individuals shall determine, with General Counsel's concurrence, which of those forms or methods require Privacy Act Statements and shall prepare the required statements. The Office of Policy requires all organizations or elements using such forms or methods shall ensure that respondents read, understand, and sign the statements before supplying the requested information. In addition, organizations must obtain the Director of Policy and the Office of General Counsel approval prior to the collection of personal information in electronic format.

§ 322.5 Procedures.

(a) The Director of Policy, or the Deputy Director of Policy, if so designated, shall provide guidance to Privacy Act Coordinators for processing requests and releasing NSA/CSS information within the confines of the NSA/CSS. If any organization or element believes a request to review a PA record should be denied, it shall advise the requester of the procedures for requesting a review of the circumstances of the case by the Director of Policy.

(b) Persons Authorized Access to NSA/CSS Facilities: (1) Requests from NSA/CSS affiliates with authorized access to NSA/CSS facilities to review and/or obtain a copy of PA records in a Systems of Records for use within NSA/CSS spaces or for the inspection of an accounting of disclosures of the record shall be in writing, using the Privacy Act Information Request form. Requests shall normally be submitted directly to the Privacy Act Coordinator in the office holding the record. In the case of requests for access to records maintained in the individual's own organization, the Privacy Act Coordinator for that organization shall direct the requester to the person or office holding the record. A Privacy Act Information Request form shall be submitted to the holder of each record desired. The Privacy Act Coordinator shall assist supervisors and record handlers in processing the request and shall maintain an accounting for reporting purposes. Individuals shall not be permitted to review or obtain an internal copy of IG, OGC and/or certain security records. The Personnel File, which was available upon request prior to the implementation of the Privacy Act, shall continue to be available for review without citing the Privacy Act or using the Privacy Act Information Request form.

(2) Requests to obtain a copy of PA records for use outside of NSA/CSS shall be forwarded to the Director of Policy, FOIA/PA Services (DC321) using the Privacy Act Information Request form or in any written format and must contain the individual's full name, signature, social security number, description of the records sought and a work or home phone number. Requests shall be processed pursuant to the Privacy Act and the FOIA.

(c) Persons Not Authorized Access to NSA/CSS Facilities: (1) Requests from individuals who do not have authorized access to NSA/CSS facilities must be in writing, contain the individual's full name, current address, signature, social security number and a description of the records sought. The mailing address for the FOIA/PA office is: National Security Agency, ATTN: FOIA/PA Services (DC321), 9800 Savage Road, Suite 6248, Ft. George G. Meade, MD 20755–6248.

(2) FOIA/PA Services may, at its discretion, require an unsworn declaration or a notarized statement of identity. In accordance with 28 U.S.C. 1746, the language for an unsworn declaration is as follows:

(i) If executed without the United States: 'I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)'.

(ii) If executed within the United States, its territories, possessions, or commonwealths: 'I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)'.

(d) General provisions regarding access and processing procedures: (1) The requester need not state a reason or otherwise justify the request. If the requester wishes to be accompanied by another person, the individual may be required to furnish a statement authorizing discussion or disclosure of the records in the presence of the other individual. If the requester wishes another person to obtain the records on

his/her behalf, the requester shall provide a written statement appointing that person as his/her representative, authorizing that individual access to the records and affirming that such access shall not constitute an invasion of the requester's privacy or a violation of his/her rights under the Privacy Act. In addition, requests from parents or legal guardians for records on a minor may be accepted providing the individual is acting on behalf of the minor and evidence is provided to support his or her parentage (birth certificate showing requester as a parent) or guardianship (a court order establishing guardianship).

(2) The Director of Policy and FOIA/PA Services (DC321) shall endeavor to respond to a direct request to the NSA/CSS within 20 working days of receipt. In the event the FOIA/PA Services cannot respond within 20 working days due to unusual circumstances, the requester shall be advised of the reason for the delay and negotiate a completion date with the requester. Direct requests to NSA/CSS shall be processed in the order in which they are received. Requests referred to NSA/CSS by other government agencies shall be placed in the processing queue according to the date the requester's letter was received by the referring agency, if that date is known. If it is not known, it shall be placed in the appropriate processing queue according to the date of the requester's letter.

(3) FOIA/PA requests for copies of records shall be worked in chronological order within six queues (''super easy,'' ''sensitive/personal easy,'' ''non-personal easy,'' ''sensitive/personal voluminous,'' ''non-personal complex,'' and ''expedite''). The processing queues are defined as follows:

(i) *Super Easy Queue*—The super easy queue is for requests for which no responsive records are located or for material that requires minimal specialized review.

(ii) *Sensitive/Personal Easy Queue*—The sensitive/personal easy queue contains FOIA and PA records that contain sensitive personal information, typically relating to the requester or requester's relatives, and that do not require a lengthy review. DC321 staff members who specialize in handling sensitive personal information process these requests.

(iii) *Non-Personal Easy Queue*—The non-personal easy queue contains all other types of NSA records not relating to the requester, that often contain classified information that may require coordinated review among NSA components, and that do not require a lengthy review. DC321 staff members who specialize in complex classification issues process these requests.

(iv) *Sensitive/Personal Voluminous Queue*—The sensitive/personal voluminous queue contains FOIA and PA records that contain sensitive personal information, typically relating to the requester or requester's relatives, and that require a lengthy review because of the high volume of responsive records. These records may also contain classified information that may require coordinated review in several NSA components. DC321 staff members who specialize in handling sensitive personal information process these requests.

(v) *Non-Personal Complex Queue*—The non-personal complex queue contains FOIA records not relating to the requester that require a lengthy review because of the high volume and/or complexity of responsive records. These records contain classified, often technical information that requires coordinated review among many specialized NSA components, as well as consultation with other government agencies. DC321 staff members who specialize in complex classification issues process these requests.

(vi) *Expedite Queue*—Cases meeting the criteria for expeditious processing as defined in this section will be processed in turn within that queue by the appropriate processing team.

(4) Requesters shall be informed immediately if no responsive records are located. Following a search for and retrieval of responsive material, the initial processing team shall determine which queue in which to place the material, based on the criteria above, and shall so advise the requester. If the material requires minimal specialized review (super easy), the initial processing team shall review, redact if required, and provide the non-exempt responsive material to the requester immediately.

The appropriate specialized processing team on a first in, first out basis within its queue shall process all other material. These procedures are followed so that a requester will not be required to wait a long period of time to learn that the Agency has no records responsive to his request or to obtain records that require minimal review.

(5) Requests for expeditious processing must include justification and a statement certifying that the information is true and correct to the best of the requester's knowledge. Expedited processing shall be granted if the requester demonstrates a compelling need for the information. Compelling need is defined as the failure to obtain the records on an expedited basis could reasonably be expected to pose an imminent threat to the life or physical safety of an individual or there would be an imminent loss of substantial due process rights.

(6) A request for expedited handling shall be responded to within 10 calendar days of receipt. The requester shall be notified whether his/her request meets the criteria for expedited processing within that time frame. If a request for expedited processing has been granted, a substantive response shall be provided within 20 working days of the date of the expedited decision. If a substantive response cannot be provided within 20 working days, a response shall be provided as soon as practicable and the chief of FOIA/PA Services shall attempt to negotiate an acceptable completion date with the requester, taking into account the number of cases preceding it in the expedite queue and the volume or complexity of the responsive material.

(7) Upon receipt of a request, FOIA/PA Services (DC321) shall review the request and direct the appropriate PA coordinator to search for responsive records. If the search locates the requested records, the PA coordinator shall furnish copies of the responsive documents to the FOIA/PA office that in turn shall make a determination as to the releasability of the records. All releasable records, or portions thereof, shall be provided to the requester. However, if information is exempt pursuant to the FOIA and PA, the requester shall be advised of the statutory basis for the denial of the information and the procedure for filing an appeal. In the instance where no responsive records are located, the requester shall be advised of the negative results and his/her right to appeal what could be considered an adverse determination. NSA does not have the authority to release another agency's information; therefore, information originated by another government agency shall be referred to the originating agency for its direct response to the requester or for review and return to NSA for response to the requester. The requester shall be advised that a referral has been made, except when notification would reveal exempt information.

(8) The requester shall not be charged a fee for the making of a comprehensible copy to satisfy the request for a copy of the documents. The requester may be charged for duplicate copies of the documents. However, if the direct cost of the duplicate copy is less than $25.00, the fee shall be waived. Duplicating fees shall be assessed according to the following schedule: Office Copy $.15 per page, Microfiche $.25 per page, and Printed Material $.02 per page. All payments shall be made by certified check or money order made payable to the Treasurer of the United States.

(9) A medical/psychological record shall normally be disclosed to the individual to whom it pertains. However, and consistent with 5 U.S.C. 552a(f)(3) of the Privacy Act, if in the judgment of an authorized Agency physician, the release of such information could have an adverse effect on the individual, the individual shall be advised that it is in his best interest to receive the records through a physician of the requester's choice or, in the case of psychological records, through a licensed Psychiatrist or licensed Clinical Psychologist of the requester's choice. NSA/CSS may require certification that the individual is licensed to practice the appropriate specialty. Although the requester shall pay any fees charged by the physician or psychologist, NSA/CSS encourages individuals to take advantage of receiving their records through this means. If, however, the individual wishes to waive receiving the records through this means, the

records shall be sent directly to the individual.

(10) Recipients of requests from NSA/CSS employees and affiliates for access to records within the confines of the NSA/CSS campus shall acknowledge the request within 10 working days of receipt, and access should be provided within 20 working days. If, for good cause, access cannot be provided within that time, the requester shall be advised in writing as to the reason and shall be given a date by which it is expected that access can be provided. If an office denies a request for access to a record, or any portion thereof, it shall notify the requester of its refusal and the reasons for it and shall advise the individual of the procedures for requesting a review of the circumstances by the Director of Policy. If the Director of Policy denies a request for access to a record or any portion thereof, the requester shall be notified of the refusal and the reasons the information was denied. The Director of Policy shall also advise the requester of the procedure for appealing to the NSA/CSS Privacy Act Appeal Authority. (*See* paragraph (e) of this section).

(11) Although classified portions of NSA/CSS records are exempt from disclosure pursuant to exemption (k)(1) of the Privacy Act and exemption (b)(1) of the FOIA, NSA, in its sole discretion, may choose to provide an NSA affiliate access to the classified portions of records about the affiliate if the affiliate possesses the requisite security clearance, special access approvals, and appropriate need-to-know for the classified information at issue. Classified records may only be accessed by fully cleared personnel in NSA/CSS spaces. Disclosure of classified records under this provision shall not operate as a waiver of PA exemption (k)(1), FOIA exemption (b)(1), or of any other exemption or privilege that would otherwise authorize the Agency to withhold the classified records from disclosure. NSA's determination regarding an affiliate's need-to-know is not subject to appeal under this or any other authority. All copies of classified records made available to an NSA affiliate under the procedures of this Part shall carry the following statement: ''This classified material is provided to you under the provisions of the Privacy Act of 1974. Furnishing you this material does not relieve you of your obligations under the laws of the United States (*See*, e.g., section 798 of Title 18, U.S. Code) to protect classified information. You may retain this material under proper protection as specified in the NSA/CSS Classification Manual; you may not remove it from NSA/CSS facilities.''

(12) The procedures described in this part do not entitle an individual to have access to any information compiled in reasonable anticipation of a civil action or proceeding, nor do they require that a record be created.

(13) Requesting or obtaining access to records under false pretenses is a violation of the Privacy Act and is subject to criminal penalties.

(e) Appeal of Denial of an Adverse Determination: (1) Any individual advised of an adverse determination shall be notified of the right to appeal the initial decision within 60 calendar days of the date of the response letter and that the appeal must be addressed to the NSA/CSS FOIA/PA Appeal Authority, National Security Agency, 9800 Savage Road, Suite 6248, Fort George G. Meade, MD 20755–6248. The following actions are considered adverse determinations:

(i) Denial of records or portions of records.

(ii) Inability of NSA/CSS to locate responsive records.

(iii) Denial of a request for expeditious treatment.

(iv) Non-agreement regarding completion date of request.

(v) The appeal shall reference the initial denial of access and shall contain, in sufficient detail and particularity, the grounds upon which the requester believes the appeal should be granted.

(2) The GC or his/her designee shall process appeals and make a recommendation to the Appeal Authority:

(i) Upon receipt of an appeal regarding the denial of information or the inability of the Agency to locate records on an individual, the GC or his/her designee shall provide a legal review of the denial and/or the adequacy of the search for responsive material, and make other recommendations as appropriate.

(ii) If the Appeal Authority determines that additional information may be released, the information shall be made available to the requester within 20 working days from receipt of the appeal. The conditions for responding to an appeal for which expedited treatment is sought by the requester are the same as those for expedited treatment on the initial processing of a request.

(iii) If the Appeal Authority determines that the denial was proper, the requester must be advised 20 days after receipt of the appeal that the appeal is denied. The requester likewise shall be advised of the basis for the denial and the provisions for judicial review of the Agency's appellate determination.

(iv) If a new search for records is conducted and produces additional records, the additional material shall be forwarded to the Director of Policy, as the initial denial authority (IDA), for review. Following review, the Director of Policy shall return the material to the GC with its recommendation for release or withholding. The GC will provide a legal review of the material, and the Appeal Authority shall make the release determination. Upon denial or release of additional information, the Appeal Authority shall advise the requester that more material was located and that the IDA and the Appeal Authority each conducted an independent review of the documents. In the case of denial, the requester shall be advised of the basis of the denial and the right to seek judicial review of the Agency's action.

(v) When a requester appeals the absence of a response to a request within the statutory time limits, the GC shall process the absence of a response as it would denial of access to records. The Appeal authority shall advise the requester of the right to seek judicial review.

(vi) Appeals shall be processed using the same multi-track system as initial requests. If an appeal cannot be responded to within 20 days, the requirement to obtain an extension from the requester is the same as with initial requests. The time to respond to an appeal, however, may be extended by the number of working days (not to exceed 10) that were not used as additional time for responding to the initial request. That is, if the initial request is processed within 20 days so that the extra 10 days of processing which an agency can negotiate with the requester are not used, the response to the appeal may be delayed for that 10 days (or any unused portion of the 10 days).

(f) Amendment of Records:

(1) Minor factual errors may be corrected without resort to the Privacy Act or the provisions of this part, provided the requester and record holder agree to that procedure. Whenever possible, a copy of the corrected record should be provided to the requester.

(2) Requests for substantive changes to include deletions, removal of records, and amendment of significant factual information, because the information is incorrect or incomplete, shall be processed under the Privacy Act and the provisions of this part. The PA amendment process is limited to correcting records that are not accurate (factually correct), relevant, timely or complete.

(3) The amendment process is not intended to replace other existing NSA/CSS Agency procedures such as those for registering grievances or appealing performance appraisal ratings. Also, since the amendment process is limited to correcting factual information, it may not be used to challenge official judgments, such as performance ratings, promotion potential, and performance appraisals as well as subjective judgments made by supervisors, which reflect his/her observations and evaluations.

(4) Requests for amendments must be in writing, include the individual's name, signature, a copy of the record under dispute or sufficient identifying particulars to permit timely retrieval of the affected record, a description of the information under dispute and evidence to support the amendment request. The mailing address for the FOIA/PA office is National Security Agency, ATTN: FOIA/PA Services (DC321), 9800 Savage Road, Suite 6248, Fort George G. Meade, MD 20755–6248. Individuals who have access to NSA/CSS spaces may send their request through the internal mail system to DC321.

(5) FOIA/PA Services (DC321) shall acknowledge the amendment request within 10 working days of receipt and respond within 30 working days. The organization/individual who originated the information under dispute shall be given 10 working days to comment. On receipt of a response, FOIA/PA Services (DC321) shall review all documentation and determine if the amendment request shall be granted. If FOIA/PA Services (DC321) agrees with the request, it shall notify the requester and the office holding the record. The latter shall promptly amend the record and notify all holders and recipients of the records of the correction. If the amendment request is denied, the requester shall be advised of the reasons for the denial and the procedures for filing an appeal.

(g) Appeal of Refusals To Amend Records—

(1) If the Director of Policy, as the Initial Denial Authority, refuses to amend any part of a record it shall notify the requester of its refusal, the reasons for the denial and the procedures for requesting a review of the decision by the NSA/CSS Appeal Authority. The Appeal Authority shall render a final decision within 30 working days, except when circumstances necessitate an extension. If an extension is necessary, the requester shall be informed, in writing, of the reasons for the delay and of the approximate date on which the review is expected to be completed. If the NSA/CSS Appeal Authority determines that the record should be amended, the requester, FOIA/PA Services, and the office holding the record will be advised. The latter shall promptly amend the record and notify all recipients.

(2) If the NSA/CSS Privacy Act Appeal Authority denies any part of the request for amendment, the requester shall be advised of the reasons for denial, his or her right to file a concise statement of reasons for disputing the information contained in the record, and his or her right to seek judicial review of the Agency's refusal to amend the record. Statements of disagreement and related notifications and summaries of the Agency's reasons for refusing to amend the record shall be processed in the manner prescribed by 32 CFR part 310.

(h) Disclosures and Accounting of Disclosures.

(1) No record contained in a System of Records maintained within the Department of Defense shall be disclosed by any means of communication to any person, or to any agency outside the Department of Defense, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record will be:

(i) To those officials and employees of the Agency who have a need for the record in the performance of their duties and the use is compatible with the purpose for which the record is maintained.

(ii) Required to be disclosed under the Freedom of Information Act, as amended.

(iii) For a routine use as described in NSA/CSS systems of records notices. The DoD ''Blanket Routine Uses'' may also apply to NSA/CSS systems of records. (*See* Appendix C to 32 CFR part 310).

(iv) To the Bureau of the Census for the purpose of planning or carrying out a census or survey or related activity authorized by law.

(v) To a recipient who has provided the Department of Defense or the Agency with advance, adequate written assurance that:

(A) The record will be used solely as a statistical research or reporting record;

(B) The record is to be transferred in a form that is not individually identifiable (*i.e.*, the identity of the individual cannot be determined by combining various statistical records); and

(C) The record will not be used to make any decisions about the rights, benefits, or entitlements of an individual.

(vi) To the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value. A record transferred to a Federal records

center for safekeeping or storage does not fall within this category since Federal records center personnel act on behalf of the Department of Defense in this instance and the records remain under the control of the NSA/CSS. No disclosure accounting record of the transfer of records to Federal records center need be maintained.

(vii) To another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the NSA/CSS specifying the particular portion and the law enforcement activity for which the record is sought. Blanket requests for all records pertaining to an individual will not be accepted. A record may also be disclosed to a law enforcement agency at the initiative of the NSA/CSS when criminal conduct is suspected, provided that such disclosure has been established in advance as a ''routine use.''

(viii) To a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of the individual to whom the record pertains.

(ix) To Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, or any joint committee of Congress or subcommittee of any such joint committee. This does not authorize the disclosure of any record subject to this part to members of Congress acting in their individual capacities or on behalf of their constituents, unless the individual consents.

(x) To the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office.

(xi) Pursuant to an order of a court of competent jurisdiction.

(A) When a record is disclosed under compulsory legal process and when the issuance of that order or subpoena is made public by the court that issued it, efforts shall be made to notify the individual to whom the record pertains. This may be accomplished by notifying the individual by mail at his most recent address as contained in the Component's records.

(B) Upon being served with an order to disclose a record, the General Counsel shall endeavor to determine whether the issuance of the order is a matter of public record and, if it is not, seek to be advised when it becomes public. An accounting of the disclosure shall be made at the time the NSA/CSS complies with the order or subpoena.

(xii) To a consumer reporting agency in accordance with section 3711(f) of Title 31.

(2) Except for disclosures made in accordance with paragraphs (h)(1)(i) and (ii) of this section, an accurate accounting of disclosures shall be kept by the record holder in consultation with the Privacy Act Coordinator.

(i) The accounting shall include the date, nature, and purpose of each disclosure of a record to any person or to another agency; and the name and address of the person or agency to whom the disclosure is made. There need not be a notation on a single document of every disclosure of a particular record, provided the record holder can construct from its System the required accounting information:

(A) When required by the individual;

(B) When necessary to inform previous recipients of any amended records, or

(C) When providing a cross reference to the justification or basis upon which the disclosure was made (including any written documentation as required in the case of the release of records for statistical or law enforcement purposes).

(ii) The accounting shall be retained for at least five years after the last disclosure, or for the life of the record, whichever is longer. No record of the disclosure of this accounting need be maintained.

(iii) Except for disclosures made under paragraph (h)(1)(vii) of this section, the accounting of disclosures shall be made available to the individual to whom the record pertains. The individual shall submit a Privacy Act Information Request form to the Privacy Act Coordinator in the office keeping the accounting of disclosures.

(3) Disclosures made under circumstances not delineated in paragraphs (h)(1)(i) through (xii) of this section shall only be made after written permission of the individual involved has been obtained. Written permission shall be recorded on or appended to the document transmitting the personal information to the other agency, in which case no separate accounting of the disclosure need be made. Written permission is required in each separate case; *i.e.,* once obtained, written permission for one case does not constitute blanket permission for other disclosures.

(4) An individual's name and address may not be sold or rented unless such action is specifically authorized by law. This provision shall not be construed to require withholding of names and addresses otherwise permitted to be made public. Lists or compilations of names and home addresses, or single home addresses will not be disclosed, without the consent of the individual involved, to the public, including, but not limited to individual Congressmen, creditors, and commercial and financial institutions. Requests for home addresses may be referred to the last known address of the individual for reply at his discretion and the requester will be notified accordingly.

§ 322.6 Establishing exemptions.

(a) Neither general nor specific exemptions are established automatically for any system of records. The head of the DoD Component maintaining the system of records must make a determination whether the system is one for which an exemption properly may be claimed and then propose and establish an exemption rule for the system. No system of records within the Department of Defense shall be considered exempted until the head of the Component has approved the exemption and an exemption rule has been published as a final rule in the FEDERAL REGISTER.

(b) No system of records within NSA/CSS shall be considered exempt under subsection (j) or (k) of the Privacy Act until the exemption rule for the system of records has been published as a final rule in the FEDERAL REGISTER.

(c) An individual is not entitled to have access to any information compiled in reasonable anticipation of a civil action or proceeding (5 U.S.C. 552a(d)(5)).

(d) Proposals to exempt a system of records will be forwarded to the Defense Privacy Office, consistent with the requirements of 32 CFR part 310, for review and action.

(e) Consistent with the legislative purpose of the Privacy Act of 1974, NSA/CSS will grant access to nonexempt material in the records being maintained. Disclosure will be governed by NSA/CSS's Privacy Regulation, but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal or civil violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered, the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of the above nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated above. The decisions to release information from these systems will be made on a case-by-case basis.

(f) Do not use an exemption to deny an individual access to any record to which he or she would have access under the Freedom of Information Act (5 U.S.C. 552).

(g) Disclosure of records pertaining to personnel, or the functions and activities of the National Security Agency shall be prohibited to the extent authorized by Pub. L. No. 86–36 (1959) and 10 U.S.C. 424.

(h) Exemptions NSA/CSS may claim.

(1) *General exemption*. The general exemption established by 5 U.S.C. 552a(j)(2) may be claimed to protect investigative records created and maintained by law enforcement activities of the NSA.

(2) *Specific exemptions*. The specific exemptions permit certain categories of records to be exempt from certain specific provisions of the Privacy Act.

(i) *(k)(1) exemption.* Information properly classified under Executive Order 12958 and that is required by Executive Order to be kept secret in the interest of national defense or foreign policy.

(ii) *(k)(2) exemption.* Investigatory information compiled for law-enforcement purposes by non-law enforcement activities and which is not within the scope of Sec. 310.51(a). If an individual is denied any right, privilege or benefit that he or she is otherwise entitled by federal law or for which he or she would otherwise be eligible as a result of the maintenance of the information, the individual will be provided access to the information except to the extent that disclosure would reveal the identity of a confidential source. This subsection when claimed allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(iii) *(k)(3) exemption.* Records maintained in connection with providing protective services to the President and other individuals identified under 18 U.S.C. 3506.

(iv) *(k)(4) exemption.* Records maintained solely for statistical research or program evaluation purposes and which are not used to make decisions on the rights, benefits, or entitlement of an individual except for census records which may be disclosed under 13 U.S.C. 8.

(v) *(k)(5) exemption.* Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information, but only to the extent such material would reveal the identity of a confidential source. This provision allows protection of confidential sources used in background investigations, employment inquiries, and similar inquiries that are for personnel screening to determine suitability, eligibility, or qualifications.

(vi) *(k)(6) exemption.* Testing or examination material used solely to determine individual qualifications for appointment or promotion in the federal or military service, if the disclosure would compromise the objectivity or fairness of the test or examination process.

(vii) *(k)(7) exemption.* Evaluation material used to determine potential for promotion in the Military Services, but only to the extent that the disclosure of such material would reveal the identity of a confidential source.

§ 322.7 Exempt systems of records.

(a) All systems of records maintained by the NSA/CSS and its components shall be exempt from the requirements of 5 U.S.C. 552a(d) pursuant to 5 U.S.C. 552a(k)(1) to the extent that the system contains any information properly classified under Executive Order 12958 and that is required by Executive Order 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) GNSA 01.

(1) *System name:* Access, Authority and Release of Information File.

(2) *Exemption:* (i) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(ii) Therefore, portions of this system may be exempt pursuant to 5 U.S.C. 552a(k)(5) from the following subsections of 5 U.S.C. 552a(c)(3), (d), and (e)(1).

(3) AUTHORITY: 5 U.S.C. 552a(k)(5).

(4) *Reasons:* (i) From subsection (c)(3) and (d) when access to accounting disclosures and access to or amendment of records would cause the identity of a confidential sources to be revealed. Disclosure of the source's identity not only will result in the Department breaching the promise of confidentiality made to the source but it will impair the Department's future ability to compile investigatory material for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access to classified information. Unless sources can be assured

that a promise of confidentiality will be honored, they will be less likely to provide information considered essential to the Department in making the required determinations.

(ii) From (e)(1) because in the collection of information for investigatory purposes, it is not always possible to determine the relevance and necessity of particular information in the early stages of the investigation. In some cases, it is only after the information is evaluated in light of other information that its relevance and necessity becomes clear. Such information permits more informed decision-making by the Department when making required suitability, eligibility, and qualification determinations.

(c) GNSA 02.

(1) *System name:* Applicants.

(2) *Exemption:* (i) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(ii) Therefore, portions of this system may be exempt pursuant to 5 U.S.C. 552a(k)(5) from the following subsections of 5 U.S.C. 552a(c)(3), (d), and (e)(1).

(3) AUTHORITY: 5 U.S.C. 552a(k)(5).

(4) *Reasons:* (i) From subsection (c)(3) and (d) when access to accounting disclosures and access to or amendment of records would cause the identity of a confidential source to be revealed. Disclosure of the source's identity not only will result in the Department breaching the promise of confidentiality made to the source but it will impair the Department's future ability to compile investigatory material for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access to classified information. Unless sources can be assured that a promise of confidentiality will be honored, they will be less likely to provide information considered essential to the Department in making the required determinations.

(ii) From (e)(1) because in the collection of information for investigatory purposes, it is not always possible to determine the relevance and necessity of particular information in the early stages of the investigation. In some cases, it is only after the information is evaluated in light of other information that its relevance and necessity becomes clear. Such information permits more informed decision-making by the Department when making required suitability, eligibility, and qualification determinations.

(d) GNSA 03.

(1) *System name:* Correspondence, Cases, Complaints, Visitors, Requests.

(2) *Exemption:* (i) Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identity of a confidential source.

NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(ii) Records maintained solely for statistical research or program evaluation purposes and which are not used to make decisions on the rights, benefits, or entitlement of an individual except for census records which may be disclosed under 13 U.S.C. 8, may be exempt pursuant to 5 U.S.C. 552a(k)(4).

(iii) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(iv) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(2), (k)(4), and (k)(5) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) AUTHORITY: 5 U.S.C. 552a(k)(2), (k)(4), and (k)(5).

(4) *Reasons:* (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(ii) From subsections (d) and (f) because providing access to records of a civil or administrative 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; enable individuals to conceal their wrongdoing or mislead the course of the investigation; 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) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because there is no necessity for such publication since the system of records will be exempt from the underlying duties to provide notification about and access to information in the system and to make amendments to and corrections of the information in the system.

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NSA will, nevertheless, continue to publish such a notice in broad generic terms, as is its current practice.

(e) GNSA 04.

(1) *System name:* Military Reserve Personnel Data Base.

(2) *Exemption:* (i) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(ii) Therefore, portions of this system may be exempt pursuant to 5 U.S.C. 552a(k)(5) from the following subsections of 5 U.S.C. 552a(c)(3), (d), and (e)(1).

(3) AUTHORITY: 5 U.S.C. 552a(k)(5).

(4) *Reasons:* (i) From subsection (c)(3) and (d) when access to accounting disclosures and access to or amendment of records would cause the identity of a confidential sources to be revealed. Disclosure of the source's identity not only will result in the Department breaching the promise of confidentiality made to the source but it will impair the Department's future ability to compile investigatory material for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access to classified information. Unless sources can be assured that a promise of confidentiality will be honored, they will be less likely to provide information considered essential to the Department in making the required determinations.

(ii) From (e)(1) because in the collection of information for investigatory purposes, it is not always possible to determine the relevance and necessity of particular information in the early stages of the investigation. In some cases, it is only after the information is evaluated in light of other information that its relevance and necessity becomes clear. Such information permits more informed decision-making

by the Department when making required suitability, eligibility, and qualification determinations.

(f) GNSA 05.

(1) *System name:* Equal Employment Opportunity Data.

(2) *Exemption:* (i) Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identity of a confidential source.

NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(ii) Records maintained solely for statistical research or program evaluation purposes and which are not used to make decisions on the rights, benefits, or entitlement of an individual except for census records which may be disclosed under 13 U.S.C. 8, may be exempt pursuant to 5 U.S.C. 552a(k)(4).

(iii) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(2) and (k)(4) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) AUTHORITY: 5 U.S.C. 552a(k)(2) and (k)(4).

(4) *Reasons:* (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(ii) From subsections (d) and (f) because providing access to records of a civil or administrative 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; enable individuals to conceal their wrongdoing or mislead the course of the investigation; 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) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because there is no necessity for such publication since the system of records will be exempt from the underlying duties to provide notification about and access to information in the system and to make amendments to and corrections of the information in the system.

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NSA will, nevertheless, continue to publish such a notice in broad generic terms, as is its current practice.

(g) GNSA 06.

(1) *System name:* Health, Medical and Safety Files.

(2) *Exemption:* (i) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(ii) Testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service may be exempt pursuant to 5 U.S.C. 552a(k)(6), if the disclosure would compromise the objectivity or fairness of the test or examination process.

(iii) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(5) and (k)(6) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) AUTHORITY: 5 U.S.C. 552a(k)(5) and (k)(6).

(4) *Reasons:* (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(ii) From subsections (d) and (f) because providing access to records of a civil or administrative 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; enable individuals to conceal their wrongdoing or mislead the course of the investigation; 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) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because there is no necessity for such publication since the system of records will be exempt from the underlying duties to provide notification about and access to information in the system and to make amendments to and corrections of the information in the system.

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NSA will, nevertheless, continue to publish such a notice in broad generic terms, as is its current practice.

(h) GNSA 08.

(1) *System name:* Payroll and Claims.

(2) *Exemption:* (i) Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identity of a confidential source.

NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(ii) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(2) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

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

(4) *Reasons:* (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(ii) From subsections (d) and (f) because providing access to records of a civil or administrative 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; enable individuals to conceal their wrongdoing or mislead the course of the investigation; 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) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because there is no necessity for such publication since the system of records will be exempt from the underlying duties to provide notification about and access to information in the system and to make amendments to and corrections of the information in the system.

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NSA will, nevertheless, continue to publish such a notice in broad generic terms, as is its current practice.

(i) GNSA 09.

(1) *System name:* Personnel File.

(2) *Exemption:* (i) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(ii) Testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service may be exempt pursuant to 5 U.S.C. 552a(k)(6), if the disclosure would compromise the objectivity or fairness of the test or examination process.

(iii) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(5) and (k)(6) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) AUTHORITY: 5 U.S.C. 552a(k)(5) and (k)(6).

(4) *Reasons:* (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(ii) From subsections (d) and (f) because providing access to records of a civil or administrative 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; enable individuals to conceal their wrongdoing or mislead the course of the investigation; 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) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because there is no necessity for such publication since the system of records will be exempt from the underlying duties to provide notification about and access to information in the system and to make amendments to and corrections of the information in the system.

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NSA will, nevertheless, continue to publish such a notice in broad generic terms, as is its current practice.

(j) GNSA 10.

(1) *System name:* Personnel Security File.

(2) *Exemption:* (i) Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identity of a confidential source.

NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(ii) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(iii) Testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service may be exempt pursuant to 5 U.S.C. 552a(k)(6), if the disclosure would compromise the objectivity or fairness of the test or examination process.

(iv) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(2), (k)(5), and (k)(6) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) AUTHORITY: 5 U.S.C. 552a(k)(2), (k)(5), and (k)(6).

(4) *Reasons:* (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(ii) From subsections (d) and (f) because providing access to records of a civil or administrative 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; enable individuals to conceal their wrongdoing or mislead the course of the investigation; 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) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in

light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because there is no necessity for such publication since the system of records will be exempt from the underlying duties to provide notification about and access to information in the system and to make amendments to and corrections of the information in the system.

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NSA will, nevertheless, continue to publish such a notice in broad generic terms, as is its current practice.

(k) GNSA 12.

(1) *System name:* Training.

(2) *Exemption:* (i) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(ii) Testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service may be exempt pursuant to 5 U.S.C. 552a(k)(6), if the disclosure would compromise the objectivity or fairness of the test or examination process.

(iii) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(5) and (k)(6) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) AUTHORITY: 5 U.S.C. 552a(k)(5), and (k)(6).

(4) *Reasons:* (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(ii) From subsections (d) and (f) because providing access to records of a civil or administrative 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; enable individuals to conceal their wrongdoing or mislead the course of the investigation; 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) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because there is no necessity for such publication since the system of records will be exempt from the underlying duties to provide notification about and access to information in the system and to make amendments to and corrections of the information in the system.

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NSA will, nevertheless, continue to publish such a notice in broad generic terms, as is its current practice.

(l) *ID:* GNSA 29 (General Exemption)

(1) *System name:* NSA/CSS Office of Inspector General Investigations and Complaints.

(2) *Exemption:* Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if any individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information except to the extent that disclosure would reveal the identity of a confidential source.

NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

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

(4) *Reasons:* (i) From subsection (c)(3) and (d) when access to accounting disclosures and access to or amendment of records would cause the identity of a confidential source to be revealed. Disclosure of the source's identity not only will result in the Department breaching the promise of confidentiality made to the source but it will impair the Department's future ability to compile investigatory material for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access to classified information. Unless sources can be assured that a promise of confidentiality will be honored, they will be less likely to provide information considered essential to the Department in making the required determinations.

(ii) From (e)(1) because in the collection of information for investigatory purposes, it is not always possible to determine the relevance and necessity of particular information in the early stages of the investigation. In some cases, it is only after the information is evaluated in light of other information that its relevance and necessity becomes clear. Such information permits more informed decision-making by the Department when making required suitability, eligibility, and qualification determinations

(m) GNSA 14.

(1) *System name:* Library Patron File Control System.

(2) *Exemption:* (i) Records maintained solely for statistical research or program evaluation purposes and which are not used to make decisions on the rights, benefits, or entitlement of an individual except for census records which may be disclosed under 13 U.S.C. 8, may be exempt pursuant to 5 U.S.C. 552a(k)(4).

(ii) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(4) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) AUTHORITY: 5 U.S.C. 552a(k)(4).

(4) *Reasons:* (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(ii) From subsections (d) and (f) because providing access to records of a civil or administrative 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; enable individuals to conceal their wrongdoing or mislead the course of the investigation; 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) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because there is no necessity for such publication since the system of records will be exempt from the underlying duties to provide notification about and access to information in the system and to make amendments to and corrections of the information in the system.

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NSA will, nevertheless, continue to publish such a notice in broad generic terms, as is its current practice.

(n) GNSA 15.

(1) *System name:* Computer Users Control System.

(2) *Exemption:* (i) Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identity of a confidential source.

NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(ii) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(2) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

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

(4) *Reasons:* (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(ii) From subsections (d) and (f) because providing access to records of a civil or administrative 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; enable individuals to conceal their wrongdoing or mislead the course of the investigation; 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) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because there is no necessity for such publication since the system of records will be exempt from the underlying duties to provide notification about and access to information in the system and to make amendments to and corrections of the information in the system.

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system

notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NSA will, nevertheless, continue to publish such a notice in broad generic terms, as is its current practice.

(o) GNSA 17.

(1) *System name:* Employee Assistance Service (EAS) Case Record System.

(2) *Exemption:* (i) Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identity of a confidential source.

NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(ii) Records maintained solely for statistical research or program evaluation purposes and which are not used to make decisions on the rights, benefits, or entitlement of an individual except for census records which may be disclosed under 13 U.S.C. 8, may be exempt pursuant to 5 U.S.C. 552a(k)(4).

(iii) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(iv) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(2), (k)(4), and (k)(5) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) AUTHORITY: 5 U.S.C. 552a(k)(2), (k)(4), and (k)(5).

(4) *Reasons:* (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(ii) From subsections (d) and (f) because providing access to records of a civil or administrative 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; enable individuals to conceal their wrongdoing or mislead the course of the investigation; 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) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because there is no necessity for such publication since the system of records will be exempt from the underlying duties to provide notification about and access to information in the system and to make amendments to and corrections of the information in the system.

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NSA will, nevertheless, continue to

publish such a notice in broad generic terms, as is its current practice.

(p) GNSA 18.

(1) *System name:* Operations Files.

(2) *Exemption:* (i) Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identity of a confidential source.

NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(ii) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(iii) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(2) and (k)(5) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) AUTHORITY: 5 U.S.C. 552a(k)(2) and (k)(5).

(4) *Reasons:* (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(ii) From subsections (d) and (f) because providing access to records of a civil or administrative 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; enable individuals to conceal their wrongdoing or mislead the course of the investigation; 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) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because there is no necessity for such publication since the system of records will be exempt from the underlying duties to provide notification about and access to information in the system and to make amendments and corrections to the information in the system.

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NSA will, nevertheless, continue to publish such a notice in broad generic terms, as is its current practice.

(q) GNSA 20.

(1) *System name:* NSA Police Operational Files.

(2) *Exemption:* (i) Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result

of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identity of a confidential source.

NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(ii) Records maintained solely for statistical research or program evaluation purposes and which are not used to make decisions on the rights, benefits, or entitlement of an individual except for census records which may be disclosed under 13 U.S.C. 8, may be exempt pursuant to 5 U.S.C. 552a(k)(4).

(iii) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(iv) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(2), (k)(4), and (k)(5) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) *Authority:* 5 U.S.C. 552a(k)(2), (k)(4), and (k)(5).

(4) *Reasons:* (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(ii) From subsections (d) and (f) because providing access to records of a civil or administrative 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; enable individuals to conceal their wrongdoing or mislead the course of the investigation; 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) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because this system of records is compiled for investigative purposes and is exempt from the access provisions of subsections (d) and (f).

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants.

(r) [Reserved]

(s) GNSA 25.

(1) *System name:* NSA/CSS Operations Travel Records.

(2) *Exemption:* (i) Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identify of a confidential source.

NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(ii) Records maintained solely for statistical research or program evaluation purposes and which are not used to

make decisions on the rights, benefits, or entitlement of an individual except for census records which may be disclosed under 13 U.S.C. 8, may be exempt pursuant to 5 U.S.C. 552a(k)(4).

(3) *Authority:* 5 U.S.C. 552a(k)(2)(k)(4).

(4) *Reasons:* (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(ii) From subsections (d) and (f) because providing access to records of a civil or administrative 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; enable individuals to conceal their wrongdoing or mislead the course of the investigation; 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) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because this system of records is compiled for investigative purposes and is exempt from the access provisions of subsections (d) and (f).

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants.

(t) GNSA 26.

(1) *System Name:* NSA/CSS Accounts Receivable, Indebtedness and Claims.

(2) *Exemption:* (i) Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identify of a confidential source.

NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(ii) Records maintained solely for statistical research or program evaluation purposes and which are not used to make decisions on the rights, benefits, or entitlement of an individual except for census records which may be disclosed under 13 U.S.C. 8, may be exempt pursuant to 5 U.S.C. 552a(k)(4).

(3) Authority: 5 U.S.C. 552a(k)(2)(k)(4).

(4) *Reasons:* (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(ii) From subsections (d) and (f) because providing access to records of a civil or administrative 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; enable individuals to conceal their wrongdoing or mislead the course of the investigation; 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) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because this system of records is compiled for investigative purposes and is exempt from the access provisions of subsections (d) and (f).

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants.

(u) ID: GNSA 28 (General Exemption)

(1) *System name:* Freedom of Information Act, Privacy Act and Mandatory Declassification Review Records.

(2) *Exemption:* During the processing of letters and other correspondence to the National Security Agency/Central Security Service, exempt materials from other systems of records may in turn become part of the case record in this system. To the extent that copies of exempt records from those ''other'' systems of records are entered into this system, the National Security Agency/Central Security Service hereby claims the same exemptions for the records from those ''other'' systems that are entered into this system, as claimed for the original primary system of which they are a part.

(3) *Authority:* 5 U.S.C. 552a(k)(2) through (k)(7).

(4) *Reasons:* During the course of a FOIA/Privacy Act and/or MDR action, exempt materials from other system of records may become part of the case records in this system of records. To the extent that copies of exempt records from those other systems of records are entered into these case records, NSA/CSS hereby claims the same exemptions for the records as claimed in the original primary system of records of which they are a part. The exemption rule for the original records will identify the specific reasons why the records are exempt from specific provisions of 5 U.S.C. 552a.

[68 FR 28757, May 27, 2003, as amended at 69 FR 62408, Oct. 26, 2004; 74 FR 55779, 55780, Oct. 29, 2009; 76 FR 22615, 22616, Apr. 22, 2011; 77 FR 15596, 15597, Mar. 16, 2012; 77 FR 19095, Mar. 30, 2012]

PART 323—DEFENSE LOGISTICS AGENCY PRIVACY PROGRAM

Sec.
323.1 Purpose.
323.2 Applicability.
323.3 Policy.
323.4 Responsibilities.
323.5 Access to systems of records information.
323.6 Exemption rules.

AUTHORITY: Privacy Act of 1974, Pub. L. 93–579, Stat. 1896 (5 U.S.C. 552a).

SOURCE: 78 FR 25854, May 3, 2013, unless otherwise noted.

§ 323.1 Purpose.

This part sets out Defense Logistics Agency policy, assigns responsibilities, and prescribes procedures for the effective administration of the DLA Privacy Program.

§ 323.2 Applicability.

This part:

(a) Applies to Defense Logistics Agency Headquarters (DLA HQ) and all other organizational entities within the Defense Logistics Agency (hereafter referred to as ''DLA Components'').

(b) Shall be made applicable by contract or other legally binding action to U.S. Government contractors whenever a DLA contract requires the performance of any activities associated with maintaining a system of records, including the collection, use, and dissemination of records on behalf of DLA.

§ 323.3 Policy.

DLA adopts and supplements the DoD Privacy Program policy and procedures codified at 32 CFR 310.4 through 310.53, and appendices A through H of 32 CFR part 310.

§ 323.4 Responsibilities.

(a) *General Counsel*. The General Counsel, DLA, under the authority of the Director, Defense Logistics Agency:

(1) Implements the DLA Privacy Program and is hereby designated as the Component Senior Official for Privacy.

(2) Serves as the DLA Final Denial Appellate Authority.

(3) Provides advice and assistance on all legal matters arising out of, or incident to, the implementation and administration of the DLA Privacy Program.

(4) Serves as the DLA focal point on Privacy Act litigation with the Department of Justice; and will advise the Defense Privacy and Civil Liberties Office on the status of DLA privacy litigation. This responsibility may be delegated.

(5) Serves as a member of the Defense Privacy Board Legal Committee. This responsibility may be delegated.

(6) Supervises and administers the DLA FOIA and Privacy Act Office (DGA) and assigned staff. This responsibility may be delegated.

(7) May exempt DLA systems of records.

(b) *Initial Denial Authority (IDA) at Headquarters DLA*. By this part, the DLA Director designates the Head of each Headquarters DLA Component as an IDA. Each Head may further delegate this responsibility to their Deputy. For the DLA General Counsel's Office, the Deputy General Counsel shall serve as the Initial Denial Authority (IDA).

(c) *DLA Privacy Act Office*. The DLA Privacy Act Office (DGA) staff:

(1) Formulates policies, procedures, and standards necessary for a uniform DLA Privacy Program.

(2) Serves as the DLA representative on the Defense Privacy Board and the Defense Data Integrity Board.

(3) Provides advice and assistance on privacy matters.

(4) Develops or compiles the rules, notices, and reports required under 32 CFR part 310.

(5) Assesses the impact of technology on the privacy of personal information.

(6) Conducts Privacy training for personnel assigned, employed, and detailed, including contractor personnel and individuals having primary responsibility for implementing the DLA Privacy Program.

(7) Develops forms used within the DLA Privacy Program. This part serves as the prescribing document for forms developed for the DLA Privacy Program.

(d) *DLA Components Heads*. The DLA Components Heads:

(1) Designate an individual as the point of contact for Privacy matters for their DLA Component and advise DGA of the name of official so designated. This individual also will serve as the Privacy Officer for the co-located tenant DLA organizations.

(2) Designate an official to serve as the initial denial authority for initial requests for access to an individual's records or amendments to records, and will advise DGA of the names of the officials so designated.

(e) *DLA Acquisition Management Directorate (J–7)*. The DLA Acquisition Management Directorate (J–7) shall be responsible for:

(1) Developing the specific DLA policies and procedures to be followed when soliciting bids, awarding contracts or administering contracts that are subject to 32 CFR 310.12.

(2) Establishing an appropriate contract surveillance program to ensure contractors comply with the procedures established in accordance with 32 CFR 310.12.

§ 323.5 Access to systems of records information.

(a) Individuals who wish to gain access to records contained in a system of records about themselves will submit their request in writing to the DLA FOIA/Privacy Act Office, Headquarters, Defense Logistics Agency, ATTN: DGA, 8725 John J. Kingman Road, Suite 1644, Fort Belvoir, VA 22060–6221. Any written request must:

(1) Identify the particular ''system(s) of records'' to be searched;

(2) Contain the information listed under the ''Notification procedure'' or ''Record access procedures'' elements of the applicable system of records notice;

(3) Verify identity when the information sought is of a sensitive nature by submitting an unsworn declaration in accordance with 28. U.S.C. 1746 or notarized signature;

(4) Adequately explain a request for expedited processing, if applicable;

(5) State whether they agree to pay fees associated with the processing of your request; and

(6) Contain a written release authority if records are to be released to a third party. Third parties could be, but are not limited to, a law firm, a Congressman's office, a union official, or a private entity.

(b) Amendment and/or Access denials will be processed in accordance with 32 CFR 310.18 and 310.19.

(c) If an individual disagrees with the initial agency determination regarding notification, access, or amendment, he may appeal by writing to the General Counsel, Defense Logistics Agency, ATTN: DGA, Suite 1644, 8725 John J. Kingman Road, Fort Belvoir, VA 22060–6221 or by emailing the appeal to *hq-foia@dla.mil* or by faxing the appeal to (703) 767–6091.

§ 323.6 Exemption rules.

(a) The Director, DLA or designee may claim an exemption from any provision of the Privacy Act from which an exemption is allowed.

(b) An individual is not entitled to access information that is compiled in reasonable anticipation of a civil action or proceeding. The term ''civil action or proceeding'' is intended to include court proceedings, preliminary judicial steps, and quasi-judicial administrative hearings or proceedings (i.e., adversarial proceedings that are subject to rules of evidence). Any information prepared in anticipation of such actions or proceedings, to include information prepared to advise DLA officials of the possible legal or other consequences of a given course of action, is protected. The exemption is similar to the attorney work-product privilege except that it applies even when the information is prepared by non-attorneys. The exemption does not apply to information compiled in anticipation of criminal actions or proceedings.

(c) Exempt Records Systems. All systems of records maintained by the Defense Logistics Agency will be exempt from the access provisions of 5 U.S.C. 552a(d) and the notification of access procedures of 5 U.S.C. 522a(e)(4)(H) pursuant to 5 U.S.C. 552a(k)(1) to the extent that the system contains any information properly classified under Executive Order 13526 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 DLA systems of records, is necessary because certain record systems not otherwise specifically designated for exemptions herein may contain isolated items of information which have been properly classified.

(d) System Identifier: S170.04 (Specific exemption).

(1) System name: Debarment and Suspension Files.

(2) Exemption: (i) Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). If an individual, however, is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible as a result of the maintenance of the information, the individual will be provided access to the information except to the extent that disclosure would reveal the identity of a confidential source. NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(ii) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(iii) The specific sections of 5 U.S.C. 552a from which the system is exempt are 5 U.S.C. 552a(c)(3), (d)(1) through (d)(4), (e)(1), (e)(4)(G), (H), and (I), and (f).

(3) Authorities: 5 U.S.C. 552a(k)(2) and (k)(5).

(4) Reasons: (i) From 5 U.S.C. 552a(c)(3), as granting access to the accounting for each disclosure, as required by the Privacy Act, including the date, nature, and purpose of each disclosure and the identity of the recipient, could alert the subject to the existence of an investigation or prosecutive interest by DLA or other agencies. This seriously could compromise case preparation by prematurely revealing its existence and nature; compromise or interfere with witnesses or making witnesses reluctant to cooperate; and lead to suppression, alteration, or destruction of evidence.

(ii) From 5 U.S.C. 552a(d)(1) through (4) and (f), as 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 an 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 to satisfy any Government claim arising from the investigation or proceeding.

(iii) From 5 U.S.C. 552a(e)(1), as it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From 5 U.S.C. 552a(e)(4)(G) and (H), as there is no necessity for such publication since the system of records would be exempt from the underlying duties to provide notification about and access to information in the system and to make amendments and corrections to the information in the system.

(v) From 5 U.S.C. 552a(e)(4)(I), as to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. DLA, nevertheless, will continue to publish such a notice in broad generic terms as is its current practice.

(e) System Identifier: S500.10 (Specific exemption).

(1) System name: Personnel Security Files.

(2) Exemption: (i) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(ii) Therefore, portions of this system may be exempt pursuant to 5 U.S.C. 552a(k)(5) from the following subsections of 5 U.S.C. 552a(c)(3), (d), and (e)(1).

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

(4) Reasons: (i) From 5 U.S.C. 552a(c)(3) and (d), when access to accounting disclosures and access to or amendment of records would cause the identity of a confidential source to be revealed. Disclosure of the source's identity not only will result in the Department breaching the promise of confidentiality made to the source but it would impair the Department's future ability to compile investigatory material for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access to classified information. Unless sources may be assured that a promise of confidentiality will be honored, they will be less likely to provide information considered essential to the Department in making the required determinations.

(ii) From 5 U.S.C. 552a(e)(1), as in the collection of information for investigatory purposes, it is not always possible to determine the relevance and necessity of particular information in the early stages of the investigation. In some cases, it is only after the information is evaluated in light of other information that its relevance and necessity becomes clear. Such information permits more informed decision-making by the Department when making required suitability, eligibility, and qualification determinations.

(f) System Identifier: S500.20 (Specific exemption).

(1) System name: Defense Logistics Agency (DLA) Criminal Incident Reporting System (DCIRS).

(2) Exemption: (i) Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). If an individual, however, is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information except to the extent that disclosure would reveal the identity of a confidential source. NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(ii) The specific sections of 5 U.S.C. 552a from which the system is to be exempted are 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), (I), and (f).

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

(4) Reasons: (i) From subsection (c)(3), as to grant access to an accounting of disclosures as required by the Privacy Act, including the date, nature, and purpose of each disclosure and the identity of the recipient, could alert the subject to the existence of the investigation or prosecutive interest by DLA or other agencies. This could seriously compromise case preparation by: Prematurely revealing its existence and nature; compromising or interfering with witnesses or making witnesses reluctant to cooperate; and leading to suppression, alteration, or destruction of evidence.

(ii) From 5 U.S.C. 552a(d) and (f), as providing access to this information could result in the concealment, destruction or fabrication of evidence and jeopardize the safety and wellbeing of informants, witnesses and their families, and law enforcement personnel and their families. Disclosure of this information also could reveal and render ineffectual investigative techniques, sources, and methods used by this component and could result in the invasion of privacy of individuals only incidentally related to an investigation. Investigatory material is exempt to the extent that the disclosure of such material would reveal the identity of a source who furnished the information to the Government under an express promise that the identity of the source would be held in confidence, or prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. This exemption will protect the identities of certain sources that would be otherwise unwilling to provide information to the Government. The exemption of the individual's right of access to his/her records and the reasons therefore necessitate the exemptions of this system of records from the requirements of the other cited provisions.

(iii) From 5 U.S.C. 552a(e)(1), as it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From 5 U.S.C. 552a(e)(4)(G), (H), and (I), as it will provide protection against notification of investigatory material 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 ongoing investigation, reveal investigatory techniques, and place in jeopardy confidential informants 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).

(g) System Identifier: S500.30 (Specific exemption).

(1) System name: Incident Investigation/Police Inquiry Files.

(2) Exemption: (i) Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). If an individual, however, is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information, except to the extent that disclosure would reveal the identity of a confidential source. NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(ii) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(iii) The specific sections of 5 U.S.C. 552a from which the system is exempt are 5 U.S.C. 552a(c)(3), (d)(1) through (d)(4), (e)(1), (e)(4)(G), (H), and (I), and (f).

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

(4) Reasons: (i) From 5 U.S.C. 552a(c)(3), because to grant access to the accounting for each disclosure as required by the Privacy Act, including the date, nature, and purpose of each disclosure and the identity of the recipient, could alert the subject to the existence of the investigation or prosecutive interest by DLA or other agencies. This could seriously compromise case preparation by: Prematurely revealing its existence and nature; compromising or interfering with witnesses or making witnesses reluctant to cooperate; and leading to suppression, alteration, or destruction of evidence.

(ii) From 5 U.S.C. 552a(d)(1) through (d)(4), and (f), as providing access to records of a civil or administrative 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; enable individuals to conceal wrongdoing or mislead the course of the investigation; and result in the secreting of or other disposition of assets that would make them difficult or impossible to reach to satisfy any Government claim arising from the investigation or proceeding.

(iii) From 5 U.S.C. 552a(e)(1), as it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From 5 U.S.C. 552a(e)(4)(G) and (H), as this system of records is compiled for law enforcement purposes and is exempt from the access provisions of 5 U.S.C. 552a(d) and (f).

(v) From 5 U.S.C. 552a(e)(4)(I), because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. DLA, nevertheless, will continue to publish such a notice in broad generic terms as is its current practice.

(h) System Identifier: S500.60 (Specific exemption).

(1) System name: Defense Logistics Agency Enterprise Hotline Program Records.

(2) Exemption: (i) Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5

U.S.C. 552a(k)(2). If an individual, however, is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information, except to the extent that disclosure would reveal the identity of a confidential source. NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(ii) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(iii) The specific sections of 5 U.S.C. 552a from which the system is exempt are 5 U.S.C. 552a(c)(3), (d)(1) through (4), (e)(1), (e)(4)(G), (H), (I), and (f).

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

(4) Reasons: (i) From subsection (c)(3), as to grant access to an accounting of disclosures as required by the Privacy Act, including the date, nature, and purpose of each disclosure and the identity of the recipient, could alert the subject to the existence of the investigation or prosecutive interest by DLA or other agencies. This could seriously compromise case preparation by prematurely revealing its existence and nature; compromise or interfere with witnesses or making witnesses reluctant to cooperate; and lead to suppression, alteration, or destruction of evidence.

(ii) From 5 U.S.C. 552a(d)(1) through (4) and (f), as providing access to records of a civil or administrative investigation, and the right to contest the contents of those records and force changes to be made to the information contained therein, would interfere seriously 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; enable individuals to conceal wrongdoing or mislead the course of the investigation; and result in the secreting of or other disposition of assets that would make them difficult or impossible to reach to satisfy any Government claim arising from the investigation or proceeding.

(iii) From 5 U.S.C. 552a(e)(1), as it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From 5 U.S.C. 552a(e)(4)(G) and (H), as this system of records is compiled for law enforcement purposes and is exempt from the access provisions of 5 U.S.C. 552a(d) and (f).

(v) From 5 U.S.C. 552a(e)(4)(I), as to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. DLA will, nevertheless, continue to publish such a notice in broad generic terms as is its current practice.

(i) System Identifier: S510.30 (Specific/General Exemption).

(1) System name: Freedom of Information Act/Privacy Act Requests and Administrative Appeal Records.

(2) Exemption: During the processing of a Freedom of Information Act/Privacy Act request (which may include access requests, amendment requests, and requests for review for initial denials of such requests), exempt materials from other systems of records may, in turn, become part of the case record in this system. To the extent that copies of exempt records from those ''other'' systems of records are entered into this system, the Defense Logistics Agency claims the same exemptions for the records from those ''other'' systems that are entered into this system, as

claimed for the original primary system of which they are a part.

(3) Authority: 5 U.S.C. 552a(j)(2), (k)(1) through (7).

(4) Reasons: Records are only exempt from pertinent provisions of 5 U.S.C. 552a to the extent such provisions have been identified and an exemption claimed for the original record and the purposes underlying the exemption for the original record still pertain to the record which is now contained in this system of records. In general, the exemptions were claimed in order to protect properly classified information relating to national defense and foreign policy; to avoid interference during the conduct of criminal, civil, or administrative actions or investigations; to ensure protective services provided the President and others are not compromised; to protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations; to preserve the confidentiality and integrity of Federal testing materials; and to safeguard evaluation materials used for military promotions when furnished by a confidential source. The exemption rule for the original records will identify the specific reasons why the records are exempt from specific provisions of 5 U.S.C. 552a.

(j) System identifier: S240.28 DoD (Specific exemption).

(1) System name: Case Adjudication Tracking System (CATS)

(2) Exemption: (i) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(ii) Therefore, portions of this system may be exempt pursuant to 5 U.S.C. 552a(k)(5) from the following subsections of 5 U.S.C. 552a(c)(3), (d)(1)(2)(3)(4), and (e)(1).

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

(4) Reasons: (i) From 5 U.S.C. 552a(c)(3) and (d)(1)(2)(3)(4), when access to accounting disclosures and access to or amendment of records would cause the identity of a confidential source to be revealed. Disclosure of the confidential source's identity not only will result in the Department breaching the express promise of confidentiality made to the source but it would impair the Department's future ability to compile investigatory material for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access to classified information. Unless sources may be assured that a promise of confidentiality will be honored, they will be less likely to provide information considered essential to the Department in making the required determinations.

(ii) From 5 U.S.C. 552a(e)(1), as in the collection of information for investigatory purposes, it is not always possible to determine the relevance and necessity of particular information in the early stages of the investigation. In some cases, it is only after the information is evaluated in light of other information that its relevance and necessity becomes clear. Such information permits more informed decision-making by the Department when making required suitability, eligibility, and qualification determinations.

[78 FR 25854, May 3, 2013, as amended at 80 FR 39381, July 9, 2015]

PART 324—DFAS PRIVACY ACT PROGRAM

Subpart A—General Information

Sec.

Subpart B—Systems of Records

Subpart C—Individual Access to Records

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

SOURCE: 61 FR 25561, May 22, 1996, unless otherwise noted.

Subpart A—General information

§ 324.1 Issuance and purpose.

The Defense Finance and Accounting Service fully implements the policy and procedures of the Privacy Act and the DoD 5400.11-R[1], 'Department of Defense Privacy Program' (see 32 CFR part 310). This regulation supplements the DoD Privacy Program only to establish policy for the Defense Finance and Accounting Service (DFAS) and provide DFAS unique procedures.

§ 324.2 Applicability and scope.

This regulation applies to all DFAS, Headquarters, DFAS Centers, the Financial System Organization (FSO), and other organizational components. It applies to contractor personnel who have entered a contractual agreement with DFAS. Prospective contractors will be advised of their responsibilities under the Privacy Act Program.

§ 324.3 Policy.

DFAS personnel will comply with the Privacy Act of 1974, the DoD Privacy Program and the DFAS Privacy Act Program. Strict adherence is required to ensure uniformity in the implementation of the DFAS Privacy Act Program and to create conditions that will foster public trust. Personal information maintained by DFAS organizational elements will be safeguarded. Information will be made available to the individual to whom it pertains to the maximum extent practicable. Specific DFAS policy is provided for Privacy Act training, responsibilities, reporting procedures and implementation requirements. DFAS Components will not define policy for the Privacy Act Program.

§ 324.4 Responsibilities.

(a) *Director, DFAS.* (1) Ensures the DFAS Privacy Act Program is implemented at all DFAS locations.

(2) The Director, DFAS, will be the Final Denial Appellate Authority. This authority may be delegated to the Director for Resource Management.

(3) Appoints the Director for External Affairs and Administrative Support, or a designated replacement, as the DFAS Headquarters Privacy Act Officer.

(b) *DFAS Headquarters General Counsel.* (1) Ensures uniformity is maintained in legal rulings and interpretation of the Privacy Act.

(2) Consults with DoD General Counsel on final denials that are inconsistent with other final decisions within DoD. Responsible to raise new legal issues of potential significance to other Government agencies.

(3) Provides advice and assistance to the DFAS Director, Center Directors, and the FSO as required, in the discharge of their responsibilities pertaining to the Privacy Act.

(4) Acts as the DFAS focal point on Privacy Act litigation with the Department of Justice.

(5) Reviews Headquarters' denials of initial requests and appeals.

(c) *DFAS Center Directors.* (1) Ensures that all DFAS Center personnel, all personnel at subordinate levels, and contractor personnel working with personal data comply with the DFAS Privacy Act Program.

(2) Serves as the DFAS Center Initial Denial Authority for requests made as a result of denying release of requested information at locations within DFAS Center authority. Initial denial authority may not be redelegated. Initial denial appeals will be forwarded to the appropriate DFAS Center marked to the attention of the DFAS Center Initial Denial Authority.

(d) *Director, FSO.* (1) Ensures that FSO and subordinate personnel and contractors working with personal data comply with the Privacy Act Program.

(2) Serves as the FSO Initial Denial Authority for requests made as a result

[1] Copies may be obtained at cost from the National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.

of denying release of requested information at locations within FSO authority. FSO Initial denial authority may not be redelegated.

(3) Appoints a Privacy Act Officer for the FSO and each Financial System Activity (FSA).

(e) *DFAS Headquarters Privacy Act Officer*. (1) Establishes, issues and updates policy for the DFAS Privacy Act Program and monitors compliance. Serves as the DFAS single point of contact on all matters concerning Privacy Act policy. Resolves any conflicts resulting from implementation of the DFAS Privacy Act Program policy.

(2) Serves as the DFAS single point of contact with the Department of Defense Privacy Office. This duty may be delegated.

(3) Ensures that the collection, maintenance, use and/or dissemination of records of identifiable personal information is for a necessary and lawful purpose, that the information is current and accurate for the intended use and that adequate security safeguards are provided.

(4) Monitors system notices for agency systems of records. Ensures that new, amended, or altered notices are promptly prepared and published. Reviews all notices submitted by the DFAS Privacy Act Officers for correctness and submits same to the Department of Defense Privacy Office for publication in the FEDERAL REGISTER. Maintains and publishes a listing of DFAS Privacy Act system notices.

(5) Establishes DFAS Privacy Act reporting requirement due dates. Compiles all Agency reports and submits the completed annual report to the Defense Privacy Office. DFAS reporting requirements are provided in appendix A to this part.

(6) Conducts annual Privacy Act Program training for DFAS Headquarters (HQ) personnel. Ensures that subordinate DFAS Center and FSO Privacy Act Officers fulfill annual training requirements.

(f) *FSO and Financial System Activities (FSAs) Legal Support*. The FSO and subordinate FSA organizational elements will be supported by the appropriate DFAS-HQ or DFAS Center General Counsel office.

(g) *DFAS Center(s) Assistant General Counsel*. (1) Ensures uniformity is maintained in legal rulings and interpretation of the Privacy Act and this regulation. Consults with the DFAS-HQ General Counsel as required.

(2) Provides advice and assistance to the DFAS Center Director and the FSA in the discharge of his/her responsibilities pertaining to the Privacy Act.

(3) Coordinates on DFAS Center and the FSA denials of initial requests.

(h) *DFAS Center Privacy Act Officer*. (1) Implements and administers the DFAS Privacy Act Program for all personnel, to include contractor personnel, within the Center, Operating Locations (OpLocs) and Defense Accounting Offices (DAOs).

(2) Ensures 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; the information is timely and accurate for its intended use; and that adequate safeguards are provided to prevent misuse of such information. Advises the Program Manager that systems notices must be published in the FEDERAL REGISTER prior to collecting or maintenance of the information. Submits system notices to the DFAS-HQ Privacy Act Officer for review and subsequent submission to the Department of Defense Privacy Office.

(3) Administratively controls and processes Privacy Act requests. Ensures that the provisions of this regulation and the DoD Privacy Act Program are followed in processing requests for records. Ensures all Privacy Act requests are promptly reviewed. Coordinates the reply with other organizational elements as required.

(4) Prepares denials and partial denials for the Center Director's signature and obtain required coordination with the assistant General Counsel. Responses will include written justification citing a specific exemption or exemptions.

(5) Prepares input for the annual Privacy Act Report as required using the guidelines provided in appendix A to this part.

(6) Conducts training on the DFAS Privacy Act Program for Center personnel.

(i) *FSO Privacy Act Officer*. (1) Implements and administers the DFAS Privacy Act Program for all personnel, to include contractor personnel, within the FSO.

(2) Ensures 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; the information is timely and accurate for its intended use; and that adequate safeguards are provided to prevent misuse of such information. Advises the Program Manager that systems notices must be published in the FEDERAL REGISTER prior to collecting or maintenance of the information. Submits system notices to the DFAS-HQ Privacy Act Officer for review and subsequent submission to the Department of Defense Privacy Office.

(3) Administratively controls and processes Privacy Act requests. Ensures that the provisions of this regulation and the DoD Privacy Act Program are followed in processing requests for records. Ensure all Privacy Act requests are promptly reviewed. Coordinate the reply with other organizational elements as required.

(4) Prepares denials and partial denials for signature by the Director, FSO and obtains required coordination with the assistant General Counsel. Responses will include written justification citing a specific exemption or exemptions.

(5) Prepares input for the annual Privacy Act Report (RCS: DD DA&M(A)1379) as required using the guidelines provided in appendix A to this part.

(6) Conducts training on the DFAS Privacy Act Program for FSO personnel.

(j) *DFAS employees*. (1) Will not disclose any personal information contained in any system of records, except as authorized by this regulation.

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

(3) Reports any disclosures of personal information from a system of records or the maintenance of any system of records not authorized by this regulation to the appropriate Privacy Act Officer for action.

(k) *DFAS system managers (SM)*. (1) Ensures adequate safeguards have been established and are enforced to prevent the misuse, unauthorized disclosure, alteration, or destruction of personal information contained in system records.

(2) Ensures that all personnel who have access to the system of records or are engaged in developing or supervising procedures for handling records are totally aware of their responsibilities to protect personal information established by the DFAS Privacy Act Program.

(3) Evaluates each new proposed system of records during the planning stage. The following factors should be considered:

(i) Relationship of data to be collected and retained to the purpose for which the system is maintained. All information must be relevant to the purpose.

(ii) The impact on the purpose or mission if categories of information are not collected. All data fields must be necessary to accomplish a lawful purpose or mission.

(iii) Whether informational needs can be met without using personal identifiers.

(iv) The disposition schedule for information.

(v) The method of disposal.

(vi) Cost of maintaining the information.

(4) Complies with the publication requirements of DoD 5400.11-R, 'Department of Defense Privacy Program' (see 32 CFR part 310). Submits final publication requirements to the appropriate DFAS Privacy Act Officer.

(l) *DFAS program manager(s)*. Reviews system alterations or amendments to evaluate for relevancy and necessity. Reviews will be conducted annually and reports prepared outlining the results and corrective actions taken to resolve problems. Reports will be forwarded to the appropriate Privacy Act Officer.

(m) *Federal government contractors.* When a DFAS organizational element contracts to accomplish an agency function and performance of the contract requires the operation of a system of records or a portion thereof, DoD 5400.11-R, 'Department of Defense Privacy Program' (see 32 CFR part 310) and this part apply. For purposes of criminal penalties, the contractor and its employees shall be considered employees of DFAS during the performance of the contract.

(1) *Contracting involving operation of systems of records.* Consistent with Federal Acquisition Regulation (FAR)[2] and the DoD Supplement to the Federal Acquisition Regulation (DFAR)[3], Part 224.1, contracts involving the operation of a system of records or portion thereof shall specifically identify the record system, the work to be performed and shall include in the solicitations and resulting contract such terms specifically prescribed by the FAR and DFAR.

(2) *Contracting.* For contracting subject to this part, the Agency shall:

(i) Informs prospective contractors of their responsibilities under the DFAS Privacy Act Program.

(ii) Establishes an internal system for reviewing contractor performance to ensure compliance with the DFAS Privacy Act Program.

(3) *Exceptions.* This rule does not apply to contractor records that are:

(i) Established and maintained solely to assist the contractor in making internal contractor management decisions, such as records maintained by the contractor for use in managing the contract.

(ii) Maintained as internal contractor employee records, even when used in conjunction with providing goods or services to the agency.

(4) *Contracting procedures.* The Defense Acquisition Regulatory Council is responsible for developing the specific policies and procedures for soliciting, awarding, and administering contracts.

(5) *Disclosing records to contractors.* Disclosing records to a contractor for use in performing a DFAS contract is considered a disclosure within DFAS. The contractor is considered the agent of DFAS when receiving and maintaining the records for the agency.

[2] Copies may be obtained at cost from the Superintendent of Documents, P.O. Box 37195, Pittsburgh, PA 15250–7954.

[3] See footnote 2 to § 324.4(m)(1)

Subpart B—Systems of Records

§ 324.5 General information.

(a) The provisions of DoD 5400.11-R, 'Department of Defense Privacy Program' (see 32 CFR part 310) apply to all DFAS systems of records. DFAS Privacy Act Program Procedural Rules, DFAS Exemption Rules and System of Record Notices are the three types of documents relating to the Privacy Act Program that must be published in the FEDERAL REGISTER.

(b) A system of records used to retrieve records by a name or some other personal identifier of an individual must be under DFAS control for consideration under this regulation. DFAS will maintain only those Systems of Records that have been described through notices published in the FEDERAL REGISTER.

(1) *First amendment guarantee.* No records will be maintained that describe how individuals exercise their rights guaranteed by the First Amendment unless maintenance of the record is expressly authorized by Statute, the individual or for an authorized law enforcement purpose.

(2) *Conflicts.* In case of conflict, the provisions of DoD 5400.11-R take precedence over this supplement or any DFAS directive or procedure concerning the collection, maintenance, use or disclosure of information from individual records.

(3) *Record system notices.* Record system notices are published in the FEDERAL REGISTER as notices and are not subject to the rule making procedures. The public must be given 30 days to comment on any proposed routine uses prior to implementing the system of record.

(4) *Amendments.* Amendments to system notices are submitted in the same manner as the original notices.

§ 324.6 Procedural rules.

DFAS procedural rules (regulations having a substantial and direct impact on the public) must be published in the

FEDERAL REGISTER first as a proposed rule to allow for public comment and then as a final rule. Procedural rules will be submitted through the appropriate DFAS Privacy Act Officer to the Department of Defense Privacy Office. Appendix B to this part provides the correct format. Guidance may be obtained from the DFAS-HQ and DFAS Center Records Managers on the preparation of procedural rules for publication.

§ 324.7 Exemption rules.

(a) *Submitting proposed exemption rules.* Each proposed exemption rule submitted for publication in the FEDERAL REGISTER must contain: The agency identification and name of the record system for which an exemption will be established; The subsection(s) of the Privacy Act which grants the agency authority to claim an exemption for the system; The particular subsection(s) of the Privacy Act from which the system will be exempt; and the reasons why an exemption from the particular subsection identified in the preceding subparagraph is being claimed. No exemption to all provisions of the Privacy Act for any System of records will be granted. Only the Director, DFAS may make a determination that an exemption should be established for a system of record.

(b) *Submitting exemption rules for publication.* Exemption rules must be published in the FEDERAL REGISTER first as proposed rules to allow for public comment, then as final rules. No system of records shall be exempt from any provision of the Privacy Act until the exemption rule has been published in the FEDERAL REGISTER as a final rule. The DFAS Privacy Act Officer will submit proposed exemption rules, in proper format, to the Defense Privacy Office, for review and submission to the FEDERAL REGISTER for publication. Amendments to exemption rules are submitted in the same manner as the original exemption rules.

(c) *Exemption for classified records.* Any record in a system of records maintained by the Defense Finance and Accounting Service which falls within the provisions of 5 U.S.C. 552a(k)(1) may be exempt from the following subsections of 5 U.S.C. 552a: (c)(3), (d), (e)(1), (e)(4)(G)-(e)(4)(I) and (f) to the extent that a record system contains any record properly classified under Executive Order 12589 and that the record is required to be kept classified in the interest of national defense or foreign policy. This specific exemption rule, claimed by the Defense Finance and Accounting Service under authority of 5 U.S.C. 552a(k)(1), is applicable to all systems of records maintained, including those individually designated for an exemption herein as well as those not otherwise specifically designated for an exemption, which may contain isolated items of properly classified information

(1) *General exemptions.* [Reserved]

(2) *Specific exemptions.* [Reserved]

Subpart C—Individual Access to Records

§ 324.8 Right of access.

The provisions of DoD 5400.11-R, 'Department of Defense Privacy Program' (see 32 CFR part 310) apply to all DFAS personnel about whom records are maintained in systems of records. All information that can be released consistent with applicable laws and regulations should be made available to the subject of record.

§ 324.9 Notification of record's existence.

All DFAS Privacy Act Officers shall establish procedures for notifying an individual, in response to a request, if the system of records contains a record pertaining to him/her.

§ 324.10 Individual requests for access.

Individuals shall address requests for access to records to the appropriate Privacy Act Officer by mail or in person. Requests for access should be acknowledged within 10 working days after receipt and provided access within 30 working days. Every effort will be made to provide access rapidly; however, records cannot usually be made available for review on the day of request. Requests must provide information needed to locate and identify the record, such as individual identifiers required by a particular system, to include the requester's full name and social security number.

§ 324.11 Denials.

Only a designated denial authority may deny access. The denial must be in writing.

§ 324.12 Granting individual access to records.

(a) The individual should be granted access to the original record (or exact copy) without any changes or deletions. A record that has been amended is considered the original.

(b) The DFAS component that maintains control of the records will provide an area where the records can be reviewed. The hours for review will be set by each DFAS location.

(c) The custodian will require presentation of identification prior to providing access to records. Acceptable identification forms include military or government civilian identification cards, driver's license, or other similar photo identification documents.

(d) Individuals may be accompanied by a person of their own choosing when reviewing the record; however, the custodian will not discuss the record in the presence of the third person without written authorization.

(e) On request, copies of the record will be provided at a cost of $.15 per page. Fees will not be assessed if the cost is less that $30.00. Individuals requesting copies of their official personnel records are entitled to one free copy and then a charge will be assessed for additional copies.

§ 324.13 Access to medical and psychological records.

Individual access to medical and psychological records should be provided, even if the individual is a minor, unless it is determined that access could have an adverse effect on the mental or physical health of the individual. In this instance, the individual will be asked to provide the name of a personal physician, and the record will be provided to that physician in accordance with guidance in Department of Defense 5400.11-R, 'Department of Defense Privacy Program' (see 32 CFR part 310).

§ 324.14 Relationship between the Privacy Act and the Freedom of Information Act.

Access requests that specifically state or reasonably imply that they are made under FOIA, are processed pursuant to the DFAS Freedom of Information Act Regulation. Access requests that specifically state or reasonably imply that they are made under the PA are processed pursuant to this regulation. Access requests that cite both the FOIA and the PA are processed under the Act that provides the greater degree of access. Individual access should not be denied to records otherwise releasable under the PA or the FOIA solely because the request does not cite the appropriate statute. The requester should be informed which Act was used in granting or denying access.

APPENDIX A TO PART 324—DFAS REPORTING REQUIREMENTS

By February 1, of each calendar year, DFAS Centers and Financial Systems Organizations will provide the DFAS Headquarters Privacy Act Officer with the following information:

1. Total Number of Requests for Access:
a. Number granted in whole:
b. Number granted in part:
c. Number wholly denied:
d. Number for which no record was found:
2. Total Number of Requests to Amend Records in the System:
a. Number granted in whole:
b. Number granted in part:
c. Number wholly denied:
3. The results of reviews undertaken in response to paragraph 3a of Appendix I to OMB Circular A-130[4].

APPENDIX B TO PART 324—SYSTEM OF RECORDS NOTICE

The following data captions are required for each system of records notice published in the FEDERAL REGISTER. An explanation for each caption is provided.

1. *System identifier*. The system identifier must appear in all system notices. It is limited to 21 positions, including agency code, file number, symbols, punctuation, and spaces.

2. *Security classification*. Self explanatory. (DoD does not publish this caption. However, each agency is responsible for maintaining the information.)

[4] Copies available from the Office of Personnel Management, 1900 E. Street, Washington, DC 20415.

3. *System name.* The system name must indicate the general nature of the system of records and, if possible, the general category of individuals to whom it pertains. Acronyms should be established parenthetically following the first use of the name (e.g., 'Field Audit Office Management Information System (FMIS)'). Acronyms shall not be used unless preceded by such an explanation. The system name may not exceed 55 character positions, including punctuation and spaces.

4. *Security classification.* This category is not published in the FEDERAL REGISTER but is required to be kept by the Headquarters Privacy Act Officer.

5. *System location.* a. For a system maintained in a single location, provide the exact office name, organizational identity, routing symbol, and full mailing address. Do not use acronyms in the location address.

b. For a geographically or organizationally decentralized system, describe each level of organization or element that maintains a portion of the system of records.

c. For an automated data system with a central computer facility and input or output terminals at geographically separate locations, list each location by category.

d. If multiple locations are identified by type of organization, the system location may indicate that official mailing addresses are published as an appendix to the agency's compilation of systems of records notices in the FEDERAL REGISTER. If no address directory is used, or if the addresses in the directory are incomplete, the address of each location where a portion of the record system is maintained must appear under the 'system location' caption.

e. Classified addresses shall not be listed but the fact that they are classified shall be indicated.

f. The U.S. Postal Service two-letter state abbreviation and the nine-digit zip code shall be used for all domestic addresses.

6. *Categories of individuals covered by the system.* Use clear, non technical terms which show the specific categories of individuals to whom records in the system pertain. Broad descriptions such as 'all DFAS personnel' or 'all employees' should be avoided unless the term actually reflects the category of individuals involved.

7. *Categories of records in the system.* Use clear, non technical terms to describe the types of records maintained in the system. The description of documents should be limited to those actually retained in the system of records. Source documents used only to collect data and then destroyed should not be described.

8. *Authority for maintenance of the system.* The system of records must be authorized by a Federal law or Executive Order of the President, and the specific provision must be cited. When citing federal laws, include the popular names (e.g., '5 U.S.C. 552a, The Privacy Act of 1974') and for Executive Orders, the official titles (e.g., 'Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons').

9. *Purpose(s).* The specific purpose(s) for which the system of records was created and maintained; that is, the uses of the records within DFAS and the rest of the Department of Defense should be listed.

10. *Routine uses of records maintained in the system, including categories of users and purposes of the uses.* All disclosures of the records outside DoD, including the recipient of the disclosed information and the uses the recipient will make of it should be listed. If possible, the specific activity or element to which the record may be disclosed (e.g., 'to the Department of Veterans Affairs, Office of Disability Benefits') should be listed. General statements such as 'to other Federal Agencies as required' or 'to any other appropriate Federal Agency' should not be used. The blanket routine uses, published at the beginning of the agency's compilation, applies to all system notices, unless the individual system notice states otherwise.

11. *Disclosure to consumer reporting agencies.* This entry is optional for certain debt collection systems of records.

12. *Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system.* This section is divided into four parts.

13. *Storage.* The method(s) used to store the information in the system (e.g., 'automated, maintained in computers and computer output products' or 'manual, maintained in paper files' or 'hybrid, maintained in paper files and in computers') should be stated. Storage does not refer to the container or facility in which the records are kept.

14. *Retrievability.* How records are retrieved from the system (e.g., 'by name,' 'by SSN,' or 'by name and SSN') should be indicated.

15. *Safeguards.* The categories of agency personnel who use the records and those responsible for protecting the records from unauthorized access should be stated. Generally the methods used to protect the records, such as safes, vaults, locked cabinets or rooms, guards, visitor registers, personnel screening, or computer 'fail-safe' systems software should be identified. Safeguards should not be described in such detail as to compromise system security.

16. *Retention and disposal.* Describe how long records are maintained. When appropriate, the length of time records are maintained by the agency in an active status, when they are transferred to a Federal Records Center, how long they are kept at the Federal Records Center, and when they are transferred to the National Archives or destroyed should be stated. If records eventually are destroyed, the method of destruction (e.g., shredding, burning, pulping, etc.) should be stated. If the agency rule is cited,

the applicable disposition schedule shall also be identified.

17. *System manager(s) and address.* The title (not the name) and address of the official or officials responsible for managing the system of records should be listed. If the title of the specific official is unknown, such as with a local system, the local director or office head as the system manager should be indicated. For geographically separated or organizationally decentralized activities with which individuals may correspond directly when exercising their rights, the position or title of each category of officials responsible for the system or portion thereof should be listed. Addresses that already are listed in the agency address directory or simply refer to the directory should not be included.

18. *Notification procedures.* Notification procedures describe how an individual can determine if a record in the system pertains to him/her. If the record system has been exempted from the notification requirements of subsection (f)(1) or subsection (e)(4)(G) of the Privacy Act, it should be so stated. If the system has not been exempted, the notice must provide sufficient information to enable an individual to request notification of whether a record in the system pertains to him/her. Merely referring to a DFAS regulation is not sufficient. This section should also include the title (not the name) and address of the official (usually the Program Manager) to whom the request must be directed; any specific information the individual must provide in order for DFAS to respond to the request (e.g., name, SSN, date of birth, etc.); and any description of proof of identity for verification purposes required for personal visits by the requester.

19. *Record access procedures.* This section describes how an individual can review the record and obtain a copy of it. If the system has been exempted from access and publishing access procedures under subsections (d)(1) and (e)(4)(H), respectively, of the Privacy Act, it should be so indicated. If the system has not been exempted, describe the procedures an individual must follow in order to review the record and obtain a copy of it, including any requirements for identity verification. If appropriate, the individual may be referred to the system manager or another DFAS official who shall provide a detailed description of the access procedures. Any addresses already listed in the address directory should not be repeated.

20. *Contesting records procedures.* This section describes how an individual may challenge the denial of access or the contents of a record that pertains to him or her. If the system of record has been exempted from allowing amendments to records or publishing amendment procedures under subsections (d)(1) and (e)(4)(H), respectively, of the Privacy Act, it should be so stated. If the system has not been exempted, this caption describes the procedures an individual must follow in order to challenge the content of a record pertaining to him/her, or explain how he/she can obtain a copy of the procedures (e.g., by contacting the Program Manager or the appropriate DFAS Privacy Act Officer).

21. *Record source categories.* If the system has been exempted from publishing record source categories under subsection (e)(4)(I) of the Privacy Act, it should be so stated. If the system has not been exempted, this caption must describe where DFAS obtained the information maintained in the system. Describing the record sources in general terms is sufficient; specific individuals, organizations, or institutions need not be identified.

22. *Exemptions claimed for the system.* If no exemption has been established for the system, indicate 'None.' If an exemption has been established, state under which provision of the Privacy Act it is established (e.g., 'Portions of this system of records may be exempt under the provisions of 5 U.S.C. 552a(k)(2).')

PART 326—NATIONAL RECONNAISSANCE OFFICE PRIVACY ACT PROGRAM

Sec.

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

SOURCE: 65 FR 20372, Apr. 17, 2000, unless otherwise noted.

§ 326.1 Purpose.

This part implements the basic policies and procedures outlined in the Privacy Act of 1974, as amended (5 U.S.C.

552a), and 32 CFR part 310; and establishes the National Reconnaissance Office Privacy Program (NRO) by setting policies and procedures for the collection and disclosure of information maintained in records on individuals, the handling of requests for amendment or correction of such records, appeal and review of NRO decisions on these matters, and the application of exemptions.

§ 326.2 Application.

Obligations under this part apply to all employees detailed, attached, or assigned to or authorized to act as agents of the National Reconnaissance Office. The provisions of this part shall be made applicable by contract or other legally binding action to government contractors whenever a contract is let for the operation of a system of records or a portion of a system of records.

§ 326.3 Definitions.

Access. The review or copying of a record or its parts contained in a system of records by a requester.

Agency. Any executive or military department, other establishment, or entity included in the definition of agency in 5 U.S.C. 522(f).

Control. Ownership or authority of the NRO pursuant to federal statute or privilege to regulate official or public access to records.

Disclosure. The authorized 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.

He, him, and himself. Generically used in this part to refer to both males and females.

Individual or requester. A living citizen of the U.S. or an alien lawfully admitted to the U.S. for permanent residence and to whom a record might pertain. The legal guardian or legally authorized agent of an individual has the same rights as the individual and may act on his behalf. No rights are vested in the representative of a dead person or in persons acting in an entrepreneurial (for example, sole proprietorship or partnership) capacity under this part.

Interested party. Any official in the executive (including military), legislative, or judicial branches of government, U.S. or foreign, or U.S. Government contractor who, in the sole discretion of the NRO, has a subject matter or physical interest in the documents or information at issue.

Maintain. To collect, use, store, disclose, retain, or disseminate when used in connection with records.

Originator. The NRO employee or contractor who created the document at issue or his successor in office or any official who has been delegated release or declassification authority pursuant to law.

Personal information. Information about any individual that is intimate or private to the individual, as distinguished from 'corporate information' which is in the public domain and related solely to the individual's official functions or public life (i.e., employee's name, job title, work phone, grade/rank, job location).

Privacy Act Coordinator. The NRO Information and Access Release Center Chief who serves as the NRO manager of the information review and release program instituted under the Privacy Act.

Record. Any item, collection, or grouping of information about an individual that is maintained by the NRO, including, but not limited to, the individual's education, financial transactions, medical history, and criminal or employment history, and that contains the individual's name or identifying number (such as Social Security or employee number), symbol, or other identifying particular assigned to the individual, such as fingerprint, voice print, or photograph. Records include data about individuals which is stored in computers.

Responsive record. Documents or records that the NRO has determined to be within the scope of a Privacy Act request.

Routine use. The disclosure of a record outside the Department of Defense (DoD) for a use that is compatible with the purpose for which the information was collected and maintained by NRO. Routine use encompasses not

only common or ordinary use, but also all the proper and necessary uses of the record even if such uses occur infrequently. All routine uses must be published in the FEDERAL REGISTER.

System managers. Officials who have overall responsibility for a Privacy Act system of records.

System notice. The official public notice published in the FEDERAL REGISTER of the existence and general content of the system of records.

System of records. A group of any records under the control of the NRO from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to that individual.

Working days. Days when the NRO is operating and specifically excludes Saturdays, Sundays, and legal public holidays.

§ 326.4 Policy.

(a) *Records about individuals—*

(1) *Collection.* The NRO will safeguard the privacy of individuals identified in its records. Information about an individual will, to the greatest extent practicable, be collected directly from the individual, and personal information will be protected from unintentional or unauthorized disclosure by treating it as marked 'For Official Use Only.' Access to personal information will be restricted to those employees whose official duties require it during the regular course of business.

(i) *Privacy Act Statement.* When an individual is requested to furnish personal information about himself for inclusion in a system of records, a Privacy Act Statement is required to enable him to make an informed decision whether to provide the information requested. A Privacy Act Statement may appear, in order of preference, at the top or bottom of a form, on the reverse side of a form, or attached to the form as a tear-off sheet.

(ii) *Social Security Numbers (SSNs).* It is unlawful for any governmental agency to deny an individual any right, benefit, or privilege provided by law because the individual refuses to provide his SSN. However, if a federal statute requires that the SSN be furnished or if the SSN is required to verify the identity of an individual in a system of records that was established and in use before January 1, 1975, this restriction does not apply. When collecting the SSN, a 'qualified' Privacy Act Statement must be provided even if the SSN will not be maintained in a system of records. The 'qualified' Privacy Act Statement shall inform the individual whether the disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

(2) *Maintenance.* The NRO will maintain in its records only such information about an individual which is accurate, relevant, timely, and necessary to accomplish a purpose which is required by statute or Executive Order. All records used by the NRO to make determinations about individuals will be maintained with such accuracy and completeness as is reasonably necessary to assure fairness to the individual.

(3) *Existence.* The applicability of the Privacy Act depends on the existence of an identifiable record. The procedures described in NRO regulations do not require that a record be created or that an individual be given access to records that are not retrieved by name or other individual identifier. Nor do these procedures entitle an individual to have access to any information compiled in reasonable anticipation of a civil action or proceeding. NRO will maintain only those systems of records that have been described through notices published in the FEDERAL REGISTER. A system of records from which records may be retrieved by a name or some other personal identifier must be under NRO control for consideration under this part.

(4) *Disposal.* The NRO will archive, dispose of, or destroy records containing personal data in a manner to prevent specific records from being readily identified or inadvertently compromised.

(b) *Evaluation of records.* Statutory authority to establish and maintain a system of records does not grant unlimited authority to collect and maintain all information which may be useful or convenient. Directorates and offices maintaining records will evaluate

each category of information in records systems for necessity and relevance prior to republication of all system notices in the FEDERAL REGISTER and during the design phase or change of a system of records. The following will be considered in the evaluation:

(1) Relationship of each item of information to the statutory purpose for which the system is maintained;

(2) Specific adverse consequences of not collecting each category of information; and

(3) Techniques for purging parts of the records.

(c) *Disclosure of records.* The NRO will provide the fullest access practicable by individuals to NRO records concerning them. Release of personal information to such individuals is not considered public release of information. Upon receipt of a written request, the NRO will release to individuals those records that are releasable and applicable to the individual making the request. Generally, information, other than that exempted by law and this part, will be provided to the individual. NRO personnel will comply with the Privacy Act of 1974, as amended, the DoD Privacy Act Program (32 CFR part 310), and the NRO Privacy Act Program. No NRO records shall be disclosed by any means of communication to any person or to any agency except pursuant to a written request by or the prior written consent of the individual to whom it pertains, unless disclosure of the record will be:

(1) To those employees of the NRO who have an official need for the record in the performance of their duties.

(2) Required to be disclosed to a member of the public under the Freedom of Information Act, as amended.

(3) For a routine use as defined in the Privacy Act.

(4) To the Census Bureau for the purpose of conducting a census or survey or related activity authorized by law.

(5) To a recipient who has provided the NRO with advance, adequate written assurance that the record will be used solely as statistical research and that the record is to be transferred in a form in which the individual is not identifiable.

(6) To the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the U. S. Government.

(7) To another agency or to an instrumentality of any governmental jurisdiction within or under the control of the U.S. for a civil or criminal law enforcement activity if such activity is authorized by law and if the head of the agency or governmental entity has made a written request to the NRO specifying the particular portion of the record and the law enforcement activity for which the record is sought (blanket requests will not be accepted); a record may also be disclosed to a law enforcement agency at the initiative of the NRO pursuant to the blanket routine use for law enforcement when criminal conduct is indicated in the record.

(8) To a person showing compelling circumstances affecting the health or safety of an individual if, upon such disclosure, notification is sent to the last known address of the individual to whom the record pertains (emergency medical information may be released by telephone).

(9) To Congress or any committee, joint committee, or subcommittee of Congress with respect to a matter under its jurisdiction. This provision does not authorize the disclosure of a record to members of Congress acting in their individual capacities or on behalf of their constituents making third party requests. However, such releases may be made pursuant to the blanket routine use for Congressional inquiries when a constituent has sought the assistance of his Congressman for the constituent's individual record(s).

(10) To the Comptroller General or any of his authorized representatives in the course of the performance of the duties of the General Accounting Office.

(11) Pursuant to an order of a court of competent jurisdiction. When the record is disclosed under compulsory legal process and when the issuance of that order or subpoena is made public by the court which issued it, the NRO will make reasonable efforts to notify the individual to whom the record pertains by mail at the most recent address contained in NRO records.

(12) To a consumer reporting agency in accordance with 31 U.S.C. 3711(f).

(d) *Allocation of resources.* NRO components shall exercise due diligence in their responsibilities under the Privacy Act and must devote a reasonable level of personnel to respond to requests on a 'first-in, first-out' basis. In allocating Privacy Act resources, the component shall consider its imposed business demands, the totality of resources available to it, the information review and release demands imposed by Congress and other governmental authorities, and the rights of the public under various disclosure laws. The PA Coordinator will establish priorities for cases consistent with established law to ensure that smaller as well as larger 'project' cases receive equitable attention.

(e) *Written permission for disclosure.* Disclosures made under circumstances not delineated in this part shall be made only if the written permission of the individual involved has been obtained. Written permission shall be recorded on or appended to the document transmitting the personal information to the other agency, in which case no separate accounting of the disclosure need be made. Written permission is required in each case; that is, once obtained, written permission for one case does not constitute blanket permission for other disclosures.

(f) *Coordination with other government agencies.* Records systems of the NRO may contain records originated by other agencies that may have claimed exemptions for them under the Privacy Act. Where appropriate, coordination will be effected with the originating agency. The NRO will comply with the instructions issued by another agency responsible for a system of records (e.g., Office of Personnel Management) in granting access to such records. Records containing information or interests of another government agency will not be released until coordination with the other agency involved. A request for information pertaining to the individual in an NRO record system received from another federal agency will be coordinated with the originating agency.

(g) *Accounting for disclosure.* Except for disclosures made under paragraphs (c)(1) and (c)(2) of this section, an accurate account of the disclosures shall be kept by the record holder in consultation with the Privacy Act Coordinator (PA Coordinator). There need not be a notation on a single document of every disclosure of a particular record. The record holder should be able to construct from its system of records the accounting information:

(1) When required by the individual to whom the record pertains, or

(2) When necessary to inform previous recipients of any amended records. The accounting shall be retained for at least five years or for the life of the record, whichever is longer, to be available for review by the subject of the record at his request except for disclosures made under paragraph (c)(7) of this section.

(h) *Application of rules.* Any request for access, amendment, correction, etc., of personal record information in a system of records by an individual to whom such information pertains will be governed by the Privacy Act of 1974, as amended, DoD regulatory authority, and this part, exclusively. Any denial or exemption of all or part of a record from access, disclosure, amendment, correction, etc., will be processed under DoD regulatory authority and this part, unless court order or other competent authority directs otherwise.

(i) *First Amendment rights.* No NRO official or component may maintain any information pertaining to the exercise by an individual of his rights under the First Amendment without the permission of that individual unless such collection is specifically authorized by statute or pertains to an authorized law enforcement activity.

(j) *Non-system information on individuals.* The following information is not considered part of personal records systems reportable under this part and may be maintained by NRO for ready identification, contact, and property control purposes only, provided it is not maintained in a system of records. If at any time the information described in this paragraph is being maintained in a system of records, the information is subject to the Privacy Act.

(1) Identification information at doorways, building directories, desks, lockers, name tags, etc.

(2) Geographical or agency contact cards.

(3) Property receipts and control logs for building passes, credentials, vehicles, etc.

(4) Personal working notes of employees that are merely an extension of the author's memory, if maintained properly, do not come under the Privacy Act. Personal notes are not considered official NRO records if they meet the following requirements:

(i) Keeping or discarding notes must be at the sole discretion of the author. Any requirement by supervising authority, whether by oral or written directive, regulation, policy, or memo to maintain such notes, likely would cause the notes to become official agency records.

(ii) Such notes must be restricted to the author's personal use as memory aids, and only the author may have access to them. Passing them to a successor or showing them to other personnel (including supporting staff such as secretaries) would likely cause them to become agency records.

(5) Rosters. The NRO has no restriction against rosters that contain only corporate information such as name, work telephone number, and position. Good recordkeeping practices dictate that only rosters that are relevant and necessary to the NRO's operations may be maintained, and therefore convenience rosters, which by definition do not satisfy the test, may not be maintained.

§ 326.5 Responsibilities.

(a) The Director, NRO (DNRO):

(1) Supervises the execution of the Privacy Act and this part within the NRO.

(2) Appoints:

(i) The Chief, Information Access and Release Center as the NRO Privacy Act Coordinator.

(ii) The Director of Security, the Director of Policy, and the NRO General Counsel as the NRO Appeals Panel; and

(iii) The Chief of Staff as the Senior Official for Privacy Policy and the Privacy Act Appeal Authority.

(b) The Privacy Act Coordinator, NRO:

(1) Establishes, issues, and updates policy for the NRO Privacy Act Program, monitors compliance, and serves as the principal NRO point of contact on all Privacy Act matters.

(2) Receives, processes, and responds to all Privacy Act requests received by the NRO, including:

(i) Granting, granting in part, or denying an initial Privacy Act request for access or amendment to a record, and notifying a requester of such actions taken in regard to that request.

(ii) Granting a requester access to all or part of a record under dispute when, after a review, a decision is made in favor of a requester.

(iii) Directing the appropriate NRO component to amend a record and advising other record holders to amend a record when a decision is made in favor of a requester.

(iv) Notifying a requester, if a request is denied, of the reasons for denial and the procedures for appeal to the Privacy Act Appeal Authority.

(v) Notifying a requester of his right to file a concise statement of his reasons for disagreement with the NRO's refusal to amend a record.

(vi) Directing that a requester's statement of reasons for the request to amend, his concise statement of disagreement with the NRO's refusal to amend a record, and the NRO's letter of denial be included in the file containing the disputed record.

(vii) Referring all appeals to the Privacy Act Appeals Panel and Appeal Authority.

(viii) Notifying a requester of any required fees and delivering such collected fees to the Comptroller.

(ix) Obtaining supplemental information from the requester when required.

(3) Serves as the NRO point of contact with the Defense Privacy Office.

(4) Reviews NRO use of records, and at least 40 calendar days prior to establishing a new agency system of records, ensures that new or amended notices are prepared and published in the FEDERAL REGISTER consistent with the requirements of 32 CFR part 310;

(5) Coordinates with forms managers to ensure that a Privacy Act Statement is on all forms or in all other

methods used to collect personal information for inclusion in any NRO records system;

(6) Prepares the NRO Privacy Act report for submission to the DoD Privacy Office and to other authorities, as required by 32 CFR part 310.

(7) Reviews all procedures, including forms, which require an individual to furnish information for conformity with the Privacy Act.

(8) Retains the accounting of disclosures for at least five years or for the life of the record, whichever is longer, to be available for review by the subject of the record at his request except for disclosures made under paragraph (c)(7) of § 326.4; and

(9) Develops and oversees Privacy Act Program training for NRO personnel.

(c) The Privacy Act Appeals Panel, NRO:

(1) Meets and reviews all denials appealed by means of the NRO internal appeals process; and

(2) Recommends a finding to the Privacy Act Appeal Authority by a majority vote of those present at the meeting and based on the written record and the panel's deliberations.

(d) The Privacy Act Appeal Authority, NRO:

(1) Determines all NRO Privacy Act appeals.

(2) Reports the determination to the PA Coordinator.

(3) Signs the final appeal letter to the requester.

(e) General Counsel, NRO:

(1) Ensures uniformity in NRO legal positions concerning the Privacy Act and reviews proposed responses to Privacy Act requests to ensure legal sufficiency, as appropriate.

(2) Consults with DoD General Counsel on final denials that may be inconsistent with other final decisions within DoD; raises new legal issues of potential significance to other government agencies.

(3) Provides advice and assistance to the DNRO, the PA Coordinator, and component Directors, as required, in the discharge of their responsibilities pertaining to the Privacy Act.

(4) Advises on all legal matters concerning the Privacy Act, including legal decisions, rulings by the Department of Justice, and actions by DoD and other commissions on the Privacy Act.

(5) Approves all Privacy Act Statements prior to their reproduction and distribution.

(6) Acts as the NRO focal point for Privacy Act litigation with the Department of Justice.

(7) Provides a status report to the Defense Privacy Office, consistent with the requirements of 32 CFR part 310, whenever an individual brings suit under subsection (g) of the Privacy Act against NRO.

(f) Chief Information Officer (CIO), NRO:

(1) Ensures that NRO systems of records databases have procedures to protect the confidentiality of personal records maintained or processed by means of automatic data processing (ADP) systems and ensures that ADP systems contain appropriate safeguards for the privacy of personnel.

(2) Coordinates with the PA Coordinator before developing or modifying CIO-sponsored ADP supported files subject to the provisions of this part.

(g) Directorate and Office Managers, NRO:

(1) Ensure that records contained in their directorate or office systems of records are disclosed only to those NRO officials or employees who require the records for official purposes.

(2) Review their own directorate and office systems of records to ensure and certify that no systems of records other than those listed in the FEDERAL REGISTER System Notices are maintained; notify the CIO and the PA Coordinator promptly whenever there are changes to processing equipment, hardware, software, or database that may require an amended system notice.

(3) Maintain only such information about an individual as is relevant and necessary to accomplish a purpose which is required by statute or Executive Order and identify the specific provision of law or Executive Order which provides authority for the maintenance of information in each system of records.

(h) System Managers, NRO:

(1) Ensure that adequate safeguards have been established and are enforced to prevent the misuse, unauthorized disclosure, alteration, or destruction of

personal information contained in system records.

(2) Ensure that all personnel who have access to the system of records, or are engaged in developing or supervising procedures for handling records, are aware of their responsibilities established by the NRO Privacy Act Program.

(3) Evaluate each system of records during the planning stage and at regular intervals. The following factors should be considered:

(i) Relationship of data to be collected and retained to the purposes for which the system is maintained (all information must be relevant and necessary to the purpose for which it is collected).

(ii) The specific impact on the purpose or mission if categories of information are not collected (all data fields must be necessary to accomplish a lawful purpose or mission).

(iii) Whether informational needs can be met without using personal identifiers.

(iv) The cost of maintaining and disposing of records within the systems of records and the length of time each item of information must be retained according to the NRO Records Control Schedule as approved by the National Archives and Records Administration.

(4) Review system alterations or amendments to evaluate for relevancy and necessity.

(i) Forms and Information Managers. All NRO individuals responsible for forms or methods used to collect personal information from individuals will:

(1) Ensure that Privacy Act Statements are on appropriate forms and that new forms have the required Privacy Act Statement.

(2) Determine, with General Counsel's concurrence, which forms require Privacy Act Statements and will prepare such statements.

(3) Assist the initiators in determining whether a form, format, questionnaire, or report requires a Privacy Act Statement. Privacy Act Statements must be complete, specific, written in plain English, and approved by the Office of General Counsel.

(j) Employees, NRO:

(1) Will be familiar with the provisions of this part regarding the maintenance of systems of records, authorized access, and authorized disclosure;

(2) Will collect, maintain, use, and/or disseminate records containing identifiable personal information only for lawful purposes; will keep the information current, complete, relevant, and accurate for its intended use; and will safeguard the records in a system and keep them the minimum time required;

(3) Will not disclose any personal information contained in any system of records, except as authorized by the Privacy Act and this part;

(4) Will maintain no system of records concerning individuals except those authorized, and will maintain no other information concerning individuals except as necessary for the conduct of business at the NRO;

(5) Will provide individuals a Privacy Act Statement when asking them to provide information about themselves. The Privacy Act Statement will include the authority under which the information is being requested, whether disclosure of the information is mandatory or voluntary, the purposes for which it is being requested, the uses to which it will be put, and the consequences of not providing the information;

(6) May not deny an individual any right or privilege provided by law because of that individual's failure to disclose his SSN unless such information is required by federal statute or disclosure was required by statute or regulations adopted prior to January 1, 1975. If disclosure of the SSN is not required, NRO directorates and offices are not precluded from requesting it from individuals; however, the Privacy Act Statement must make clear that the disclosure of the SSN is voluntary and, if the individual refuses to disclose it, must be prepared to identify him by alternate means.

(7) Will collect personal information directly from the subject whenever possible; employees may collect information from third parties when that information must be verified, opinions or evaluations are required, the subject cannot be contacted, or the subject requests it.

(8) Will keep paper and electronic records which contain personal information and are retrieved by name or personal identifier only in approved systems published in the FEDERAL REGISTER.

(9) Will amend and correct records when directed by the PA Coordinator.

(10) Will report to the PA Coordinator any disclosures of personal information from a system of records, or the maintenance of any system of records, not authorized by this part.

(11) Will participate in specialized Privacy Act training should their duties require dealing with special investigators, the news media, or the public.

[65 FR 20372, Apr. 17, 2000, as amended at 66 FR 41783, Aug. 9, 2001]

§ 326.6 Policies for processing requests for records.

(a) An individual's written request for access to records about himself which does not specify the Act under which the request is made will be processed under both the Freedom of Information Act (FOIA) and the Privacy Act and the applicable regulations. Such requests will be processed under both Acts regardless of whether the requester cites one Act, both, or neither in the request in order to ensure the maximum possible disclosure to the requester. Individuals may not be denied access to a record pertaining to themselves merely because those records are exempt from disclosure under the FOIA.

(b) A Privacy Act request that neither specifies the system(s) of records to be searched nor identifies the substantive nature of the information sought will be processed by searching the systems of records categorized as Environmental Health, Safety and Fitness, FOIA/Privacy, General, and Security.

(c) A Privacy Act request that does not designate the system(s) of records to be searched but does identify the substantive nature of the information sought will be processed by searching those systems of records likely to have information similar to that sought by the requester.

(d) The NRO will not disclose any record to any person or government agency except by written request or prior written consent of the subject of the record unless the disclosure is required by law or is within the exceptions of the Privacy Act. If a requester authorizes another individual to obtain the requested records on his behalf, the requester shall provide a written, signed, notarized statement appointing that individual as his representative and certifying that the individual appointed may have access to the requester's records and that such access shall not constitute an invasion of his privacy nor a violation of his rights under the Privacy Act. In lieu of a notarized statement, the NRO will accept a declaration in accordance with 28 U.S.C. 1746.

(e) Upon receipt of a written request, the Privacy Act Coordinator (PA Coordinator) will release to the requester those records which are releasable and applicable to the individual making the request. Records about individuals include data stored electronically or in electronic media. Documentary material qualifies as a record if the record is maintained in a system of records.

(f) Initial availability, potential for release, and cost determination will usually be made within ten working days of the date on which a written request for any identifiable record is received by the NRO (and acknowledgement is sent to the individual). If additional time is needed due to unusual circumstances, a written notification of the delay will be forwarded to the requester within the ten working day period. This notification will briefly explain the circumstances for the delay and indicate the anticipated date for a substantive response.

(g) All requests will be handled in the order received on a 'first-in, first-out' basis. Requests will be considered for expedited processing only if the NRO determines that there is a genuine health, humanitarian, or due process reason involving possible deprivation of life or liberty which creates an exceptional and urgent need, that there is no alternative forum for the records sought, and that substantive records relevant to the stated needs may exist and be releasable.

(h) Records provided or originated by another agency or containing other

agency information will not be released prior to coordination with the other agency involved.

(i) Requesting or obtaining access to records under false pretenses is a violation of the Privacy Act and is subject to criminal penalties.

§ 326.7 Procedures for collection.

(a) To the maximum extent practical, personal information about an individual will be obtained directly from that individual.

(b) Whenever an individual is asked to provide personal information, including Social Security Number (SSN) or a personal identifier, about himself, a Privacy Act Statement will be furnished that will advise him of the authority (whether by statute or by Executive Order) under which the information is requested, whether disclosure of the information is voluntary or mandatory, the purposes for which it is requested, the uses to which it will be put, and the consequences of not providing the information.

(c) When asking third parties to provide information about other individuals, NRO employees will advise them:

(1) Of the purpose of the request, and

(2) That their identities and the information they are furnishing may be released to the individual unless they expressly request confidentiality. All persons interviewed must be informed of their rights and offered confidentiality.

§ 326.8 Procedures for requesting access.

(a) *Request in writing.* An individual seeking notification of whether a system of records contains a record pertaining to him, or an individual seeking access to records pertaining to him which are available under the Privacy Act, shall address the request in writing to the Privacy Act Coordinator, National Reconnaissance Office, 14675 Lee Road, Chantilly, VA 20151–1715. The request should contain at least the following information:

(1) *Identification.* Reasonable identification, including first name, middle name or initial, surname, any aliases or nicknames, Social Security Number, and return address of the individual concerned, accompanied by a signed notarized statement that such information is true under penalty of perjury and swearing to or affirming his identity. An unsworn declaration, under 28 U.S.C. 1746, also is acceptable. In the case of a request for records of a sensitive nature if the PA Coordinator determines that this information does not sufficiently identify the individual, the PA Coordinator may requests additional identification or clarification of information submitted by the individual.

(i) In addition, an alien lawfully admitted for permanent residence shall provide his Alien Registration Number and the date that status was acquired.

(ii) The parent or guardian of a minor or of a person judicially determined to be incompetent, or an attorney retained to represent an individual, in addition to establishing the identity of the minor or person represented as required in this part, shall provide evidence of his own identity as required in this part and evidence of such parentage, guardianship, or representation by submitting a certified copy of the minor's birth certificate, the court order establishing such guardianship, or the representation agreement which establishes the relationship.

(2) *Cost.* A statement of willingness to pay reproduction costs. Processing of requests and administrative appeals from individuals who owe outstanding fees will be held in abeyance until such fees are paid.

(3) *Record sought.* A description, to the best of his ability, of the nature of the record sought and the system in which it is thought to be included. In lieu of this, a requester may simply describe why and under what circumstances he believes that the NRO maintains responsive records; the NRO will undertake the appropriate searches.

(b) *Access on behalf of the individual.* If the requester wishes another person to obtain the records on his behalf, the requester will furnish a notarized statement or unsworn declaration appointing that person as his representative, authorizing him access to the record, and affirming that access will not constitute an invasion of the requester's privacy or a violation of his rights

under the Privacy Act. The NRO requires a written statement to authorize discussion of the individual's record in the presence of a third person.

§ 326.9 Procedures for disclosure of requested information.

(a) The PA Coordinator shall acknowledge receipt of the request in writing within ten working days.

(b) Upon receipt of a request, the PA Coordinator shall refer the request to those components most likely to possess responsive records. The components shall search all relevant record systems within their cognizance and shall:

(1) Determine whether a responsive record exists in a system of records.

(2) Determine whether access must be denied and on what legal basis. An individual may be denied access to his records under the Privacy Act only if an exemption has been properly claimed for all or part of the records or information requested; or if the information was compiled in reasonable anticipation of a civil action or proceeding.

(3) Approve the disclosure of records for which they are the originator.

(4) Forward to the PA Coordinator all records approved for release or necessary for coordination with or referral to another originator or interested party as well as notification of the specific determination for any denial.

(c) When all records have been collected, the PA Coordinator shall notify the individual of the determination and shall provide an exact copy of records deemed to be accessible if a copy has been requested.

(d) When an original record is illegible, incomplete, or partially exempt from release, the PA Coordinator shall explain in terms understood by the requester the portions of a record that are unclear.

(e) If access to requested records, or any portion thereof, is denied, the PA Coordinator shall inform the requester in writing of the specific reason(s) for denial, including the specific citation to appropriate sections of the Privacy Act or other statutes, this and other NRO regulations, or the Code of Federal Regulations authorizing denial, and the right to appeal this determination through the NRO appeal procedure within 60 calendar days. The denial shall include the date of denial, the name and title/position of the denial authority, and the address of the NRO Appeal Authority. Access may be refused when the records are exempt by the Privacy Act. Usually an individual will not be denied access to the entire record, but only to those portions to which the denial of access furthers the purpose for which an exemption was claimed.

§ 326.10 Procedures to appeal denial of access to requested record.

(a) Any individual whose request for access is denied may request a review of the initial decision within 60 calendar days of the date of the notification of denial of access by appealing within the NRO internal appeals process. If a requester elects to request NRO review, the request shall be sent in writing to the Privacy Act Coordinator, National Reconnaissance Office, 14675 Lee Road, Chantilly, VA 20151–1715, briefly identifying the particular record which is the subject of the request and setting forth the reasons for the appeal. The request should enclose a copy of the denial correspondence. The following procedures apply to appeals within the NRO:

(1) The PA Coordinator, after acknowledging receipt of the appeal, shall promptly refer the appeal to the record-holding components, informing them of the date of receipt of the appeal and requesting that the component head or his designee review the appeal.

(2) The record-holding components shall review the initial denial of access to the requested records and shall inform the PA Coordinator of their review determination.

(3) The PA Coordinator shall consolidate the component responses, review the record, direct such additional inquiry or investigation as is deemed necessary to make a fair and equitable determination, and make a recommendation to the NRO Appeals Panel, which makes a recommendation to the Appeal Authority.

(4) The Appeal Authority shall notify the PA Coordinator of the result of the determination on the appeal, who shall

notify the individual of the determination in writing.

(5) If the determination reverses the initial denial, the PA Coordinator shall provide a copy of the records requested. If the determination upholds the initial denial, the PA Coordinator shall inform the requester of his right to judicial review in U.S. District Court and shall include the exact reasons for denial with specific citations to the provisions of the Privacy Act, other statutes, NRO regulations, or the Code of Federal Regulations upon which the determination is based.

(b) The Appeal Authority shall act on the appeal or provide a notice of extension within 30 working days.

§ 326.11 Special procedures for disclosure of medical and psychological records.

When requested medical and psychological records are not exempt from disclosure, the PA Coordinator may determine which non-exempt medical or psychological records should not be sent directly to the requester because of possible harm or adverse impact to the requester or another person. In that event, the information may be disclosed to a physician named by the requester. The appointment of the physician will be in the same notarized form or declaration as described in §326.8 and will certify that the physician is licensed to practice in the appropriate specialty (medicine, psychology, or psychiatry). Upon designation, verification of the physician's identity, and agreement by the physician to review the documents with the requester to explain the meaning of the documents and to offer counseling designed to mitigate any adverse reaction, the NRO will forward such records to the designated physician. If the requester refuses or fails to designate a physician, the record shall not be provided. Under such circumstances refusal of access is not considered a denial for Privacy Act reporting purposes. However, if the designated physician declines to furnish the records to the individual, the PA Coordinator will take action to ensure that the records are provided to the individual.

§ 326.12 Procedures to request amendment or correction of record.

(a) An individual may request amendment or correction of a record pertaining to him/her by addressing such request in writing, to the Privacy Act Coordinator, National Reconnaissance Office, 14675 Lee Road, Chantilly, VA 20151–1715. Incomplete or inaccurate requests will not be rejected categorically; instead, the requester will be asked to clarify the request as needed. A request will not be rejected or require resubmission unless additional information is essential to process the request. Usually, amendments under this part are limited to correcting factual errors and not matters of official judgment, such as promotion ratings and job performance appraisals. The requester must adequately support his claim and must identify:

(1) The particular record he wishes to amend or correct, specifying the number of pages and documents, the titles of the documents, form numbers if any, dates on documents, and individuals who signed them. Any reasonable description of the documents is acceptable. A clear and specific description of passages, pages, or documents to be amended will expedite processing the request.

(2) The desired amending language. The requester should specify the type of amendment, including complete removal of data, passages, or documents from record or correction of information to make it accurate, more timely, complete, or relevant.

(3) A justification for such amendment or correction to include any documentary evidence supporting the request.

(b) Individuals will be required to provide verification of identity as in §326.8. to ensure that the requester is seeking to amend records pertaining to himself and not, inadvertently or intentionally, the records of another individual.

(c) Minor factual errors in an individual's personal record may be corrected routinely upon request without resort to the Privacy Act or the provisions of this part, if the requester and the record holder agree to that procedure and the requester receives a copy of the corrected record whenever possible. A

written request is not required when individuals indicate amendments during routine annual review and updating of records programs conducted by the NRO for civilian personnel and the Services for military personnel. Requests for deletion, removal of records, and amendment of substantive factual information will be processed according to the Privacy Act and the provisions of this part.

(d) The PA Coordinator shall acknowledge receipt of the request in writing within ten working days. No separate acknowledgement of receipt is necessary if the request can be either approved or denied and the requester advised within the ten-day period. For written requests presented in person, written acknowledgement may be provided at the time the request is presented.

(e) The PA Coordinator shall refer such request to the record-holder components, shall advise those components of the date of receipt, and shall request that those components make a prompt determination on such request.

(f) The record-holder components shall promptly:

(1) Make any amendment or correction to any portion of the record which the individual believes is not accurate, relevant, timely, or complete and notify the PA Coordinator and all holders and recipients of such records and their amendments that the correction was made; or

(2) Set forth the reasons for the refusal, if they determine that the requested amendment or correction will not be made or if they decline to make the requested amendment but instead augment the official record, and so inform the PA Coordinator.

(g) The Privacy Act Coordinator shall:

(1) Inform the requester of the agency's determination to make the amendment or correction as requested and notify all prior recipients of the change to the disputed records for which an accounting had been required; or

(2) Inform the requester of the specific reasons and legal authorities for the agency's refusal and the procedures established for him to request a review of that refusal.

(h) The amendment procedure is not intended to replace other existing procedures such as those for registering grievances or appealing performance appraisal reports. In such cases the requester will be apprised of the appropriate procedures for such actions.

(i) This part does not permit the alteration of evidence presented to courts, boards, or other official proceedings.

§ 326.13 Procedures to appeal denial of amendment.

(a) Any individual whose request for amendment or correction is denied may request a review of the initial decision within 60 calendar days of the date of the notification of denial by appealing within the NRO internal appeals process. If a requester elects to request NRO review, the request shall be sent in writing to the Privacy Act Coordinator, National Reconnaissance Office, 14675 Lee Road, Chantilly, VA 20151–1715, briefly identifying the particular record which is the subject of the request and setting forth the reasons for the appeal. The request should enclose a copy of the denial correspondence. The following procedures apply to appeals within the NRO:

(1) The PA Coordinator, after acknowledging receipt of the appeal, shall promptly refer the appeal to the record-holding components, informing them of the date of receipt of the appeal and requesting that the component head or his designee review the appeal.

(2) The record-holding components shall review the initial denial of access to the requested records and shall inform the PA Coordinator of their review determination.

(3) The PA Coordinator shall act as secretary of the Appeals Panel. He shall:

(i) Consolidate the component responses and reasons for the initial denial.

(ii) Provide all supporting materials both furnished to and by the requester and the record-holding component.

(iii) Review the record.

(iv) Direct such additional inquiry or investigation as is deemed necessary to make a fair and equitable determination.

(v) Prepare the record and schedule the appeal for the next meeting of the Appeals Panel. The Appeals Panel shall recommend a finding to the Appeal Authority by a majority vote of those present at the meeting based on the written record and the Panel's deliberations. No personal appearances shall be permitted without the express permission of the Panel.

(4) The Appeal Authority shall notify the PA Coordinator of the result of the determination on the appeal who shall notify the individual of the determination in writing.

(5) The Appeal Authority will notify the PA Coordinator if the determination is that the record should be amended. The PA Coordinator will promptly advise the requester and the office holding the record to amend the record and to notify all prior recipients of the records for which an accounting was required of the change.

(6) If the determination upholds the initial denial, in whole or in part, the PA Coordinator shall inform the requester:

(i) Of the denial and the reason.

(ii) Of his right to file in NRO records within 60 calendar days a concise statement of the reasons for disputing the information contained in the record. If the requester elects to file a statement of disagreement, the PA Coordinator will be responsible for clearly noting any portion of the record that is disputed and for appending into the file the requester's statement as well as a copy of the NRO's letter to the requester denying the disputed information, if appropriate. The requester's statement and the NRO denial letter will be made available to anyone to whom the record is subsequently disclosed, and prior recipients of the disputed record will be provided a copy of both to the extent that an accounting of disclosures is maintained.

(iii) Of his right to judicial review in U.S. District Court.

(7) The Appeal Authority shall act on the appeal or provide a notice of extension within 30 working days.

§ 326.14 Disclosure of records to person other than subject.

(a) Personal records contained in a Privacy Act system of records maintained by NRO shall not be disclosed by any means to any person or agency outside the NRO except with the written consent of the individual subject of the record, unless as provided in this part.

(b) Except for disclosure made to members of the NRO 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 NRO systems of records and of all disclosures of investigative information. Accounting entries will record the date, kind of information, purpose of each disclosure, and the name and address of the person or agency to whom the disclosure is made. Accounting records will be maintained for at least five years after the last disclosure or for the life of the record, whichever is longer. Subjects of NRO records will be given access to associated accounting records upon request except for disclosures made pursuant to §326.4, or where an exemption has been properly claimed for the system of records.

§ 326.15 Fees.

Individuals requesting copies of their official personnel records are entitled to one free copy; a charge will be assessed for additional copies. There is a cost of $.15 per page. Fees will not be assessed if the cost is less than $30.00. Fees should be paid by check or postal money order payable to the Treasurer of the United States and forwarded to the Privacy Act Coordinator, NRO, at the time the copy of the record is delivered. In some instances, fees will be due in advance.

§ 326.16 Penalties.

Each request shall be treated as a certification by the requester that he is the individual named in the request. The Privacy Act provides criminal penalties for any person who knowingly and willfully requests or obtains any information concerning an individual under false pretenses.

§ 326.17 Exemptions.

(a) All systems of records maintained by the NRO shall be exempt from the requirements of 5 U.S.C. 552a(d) pursuant to 5 U.S.C. 552a(k)(1) to the extent

that the system contains any information properly classified under Executive Order 12958 and which is required by the Executive Order to be withheld in the interest of national defense of 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 herein may contain items of information that have been properly classified.

(b) No system of records within the NRO shall be considered exempt under subsection (j) or (k) of the Privacy Act until the exemption and the exemption rule for the system of records has been published as a final rule in the FEDERAL REGISTER.

(c) An individual is not entitled to have access to any information compiled in reasonable anticipation of a civil action or proceeding (5 U.S.C. 552a(d)(5)).

(d) Proposals to exempt a system of records will be forwarded to the Defense Privacy Office, consistent with the requirements of 32 CFR part 310, for review and action.

(e) QNRO–23.

(1) *System name:* Counterintelligence Issue Files.

(2) *Exemptions:* (i) Investigatory material compiled for law enforcement purposes may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source.

(ii) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(iii) Therefore, portions of this system of records may be exempt pursuant to 5 U.S.C. 552a(k)(2) and/or (k)(5) from the following subsections of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H) and (I), and (f).

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

(4) *Reasons:* (i) From subsection (c)(3) because to grant access to the accounting for each disclosure as required by the Privacy Act, including the date, nature, and purpose of each disclosure and the identity of the recipient, could alert the subject to the identity of the recipient, could alert the subject to the existence of the investigation or prosecutable interest by NRO or other agencies. This could seriously compromise case preparation by prematurely revealing its existence and nature; compromise or interfere with witnesses or make witnesses reluctant to cooperate; and lead to suppression, alteration, or destruction of evidence.

(ii) From subsections (d)(1) through (d)(4), and (f) because providing access to records of a civil or administrative 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; enable individuals to conceal their wrongdoing or mislead the course of the investigation; 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) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because this system of records is compiled for law enforcement purposes and is exempt from the access provisions of subsections (d) and (f).

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NRO will, nevertheless, continue to publish such a notice in broad generic terms as is its current practice.

(vi) Consistent with the legislative purpose of the Privacy Act of 1974, the NRO will grant access to nonexempt material in the records being maintained. Disclosure will be governed by NRO's Privacy Regulation, but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered, the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of the above nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated above. The decisions to release information from these systems will be made on a case-by-case basis.

(f) *QNRO–10, Inspector General Investigative Files*—(1) Exemption: This system may be exempt pursuant to 5 U.S.C. 552a(j)(2) if the information is compiled and maintained by a component of the agency which performs as its principle function any activity pertaining to the enforcement of criminal laws. Any portion of this system which falls within the provisions of 5 U.S.C. 552a(j)(2) may be exempt from the following subsections of 5 U.S.C. 552a (c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (H), and (I), (e)(5), (e)(8), (f), and (g).

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

(3) *Reasons.* (i) From subsection (c)(3) because the release of accounting of disclosure would inform a subject that he or she is under investigation. This information would provide considerable advantage to the subject in providing him or her with knowledge concerning the nature of the investigation and the coordinated investigative efforts and techniques employed by the cooperating agencies. This would greatly impede the NRO IG's criminal law enforcement.

(ii) From subsection (c)(4) and (d), because notification would alert a subject to the fact that an open investigation on that individual is taking place, and might weaken the on-going investigation, reveal investigative techniques, and place confidential informants in jeopardy.

(iii) From subsection (e)(1) because the nature of the criminal and/or civil investigative function creates unique problems in prescribing a specific parameter in a particular case with respect to what information is relevant or necessary. Also, due to NRO IG's close liaison and working relationships with other Federal, state, local and foreign country law enforcement agencies, information may be received which may relate to a case under the investigative jurisdiction of another agency. The maintenance of this information may be necessary to provide leads for appropriate law enforcement purposes and to establish patterns of activity, which may relate to the jurisdiction of other cooperating agencies.

(iv) From subsection (e)(2) because collecting information to the fullest extent possible directly from the subject individual may or may not be practical in a criminal and/or civil investigation.

(v) From subsection (e)(3) because supplying an individual with a form containing a Privacy Act Statement would tend to inhibit cooperation by many individuals involved in a criminal and/or civil investigation. The effect would be somewhat adverse to established investigative methods and techniques.

(vi) From subsection (e)(4) (G) through (I) because this system of records is exempt from the access provisions of subsection (d).

(vii) From subsection (e)(5) because the requirement that records be maintained with attention to accuracy, relevance, timeliness, and completeness

would unfairly hamper the investigative process. It is the nature of law enforcement for investigations to uncover the commission of illegal acts at diverse stages. It is frequently impossible to determine initially what information is accurate, relevant, timely, and least of all complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light.

(viii) From subsection (e)(8) because the notice requirements of this provision could present a serious impediment to law enforcement by revealing investigative techniques, procedures, and existence of confidential investigations.

(ix) From subsection (f) because the agency's rules are inapplicable to those portions of the system that are exempt and would place the burden on the agency of either confirming or denying the existence of a record pertaining to a requesting individual might in itself provide an answer to that individual relating to an on-going investigation. The conduct of a successful investigation leading to the indictment of a criminal offender precludes the applicability of established agency rules relating to verification of record, disclosure of the record to that individual, and record amendment procedures for this record system.

(x) From subsection (g) because this system of records should be exempt to the extent that the civil remedies relate to provisions of 5 U.S.C. 552a from which this rule exempts the system.

(4) *Exemptions.* (i) Investigative material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source.

(ii) Investigative material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(iii) Therefore, portions of this system of records may be exempt pursuant to 5 U.S.C. 552a(k)(2) and/or (k)(5) from the following subsections of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H) and (I), and (f).

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

(6) *Reasons.* (i) From subsection (c)(3) because to grant access to the accounting for each disclosure as required by the Privacy Act, including the date, nature, and purpose of each disclosure and the identity of the recipient, could alert the subject to the existence of the investigation or prosecutable interest by the NRO or other agencies. This could seriously compromise case preparation by prematurely revealing its existence and nature; compromise or interfere with witnesses or make witnesses reluctant to cooperate; and lead to suppression, alteration, or destruction of evidence.

(ii) From subsections (d) and (f) because providing access to investigative records 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; enable individuals to conceal their wrongdoing or mislead the course of the investigation; 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) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because this system of records is compiled for investigative purposes and is exempt from the access provisions of subsections (d) and (f).

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NRO will, nevertheless, continue to publish such a notice in broad generic terms as is its current practice.

(vi) Consistent with the legislative purpose of the Privacy Act of 1974, the NRO will grant access to nonexempt material in the records being maintained. Disclosure will be governed by NRO's Privacy Regulation, but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal or civil violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered, the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of the above nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated above. The decisions to release information from these systems will be made on a case-by-case basis.

(g) QNRO–15, Facility Security Files.

(1) *Exemptions.* (i) Investigative material compiled for law enforcement purposes may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source.

(ii) Investigative material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(iii) Therefore, portions of this system of records may be exempt pursuant to 5 U.S.C. 552a(k)(2) and/or (k)(5) from the following subsections of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H) and (I), and (f).

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

(3) *Reasons.* (i) From subsection (c)(3) because to grant access to the accounting for each disclosure as required by the Privacy Act, including the date, nature, and purpose of each disclosure and the identity of the recipient, could alert the subject to the existence of the investigation or prosecutable interest by the NRO or other agencies. This could seriously compromise case preparation by prematurely revealing its existence and nature; compromise or interfere with witnesses or make witnesses reluctant to cooperate; and lead to suppression, alteration, or destruction of evidence.

(ii) From subsections (d)(1) through (d)(4), and (f) because providing access to investigative records 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;

enable individuals to conceal their wrongdoing or mislead the course of the investigation; 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) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because this system of records is compiled for investigative purposes and is exempt from the access provisions of subsections (d) and (f).

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NRO will, nevertheless, continue to publish such a notice in broad generic terms as is its current practice.

(vi) Consistent with the legislative purpose of the Privacy Act of 1974, the NRO will grant access to nonexempt material in the records being maintained. Disclosure will be governed by NRO's Privacy Regulation, but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal or civil violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered; the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of the above nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated above. The decisions to release information from these systems will be made on a case-by-case basis.

(h) QNRO–19.

(1) *System name:* Customer Security Services Personnel Security Files.

(2) *Exemptions:* (i) Investigatory material compiled for law enforcement purposes may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source.

(ii) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(iii) Therefore, portions of this system of records may be exempt pursuant to 5 U.S.C. 552a(k)(2) and/or (k)(5) from the following subsections of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H) and (I), and (f).

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

(4) *Reasons:* (i) From subsection (c)(3) because to grant access to the accounting for each disclosure as required by the Privacy Act, including the date, nature, and purpose of each disclosure and the identity of the recipient, could alert the subject to the existence of the investigation or prosecutable interest by the NRO or other agencies. This could seriously compromise case preparation by prematurely revealing its existence and nature; compromise or interfere with witnesses or make witnesses reluctant to cooperate; and lead to suppression, alteration, or destruction of evidence.

(ii) From subsections (d)(1) through (d)(4), and (f) because providing access to investigatory records 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; enable individuals to conceal their wrongdoing or mislead the course of the investigation; 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) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because this system of records is compiled for investigatory purposes and is exempt from the access provisions of subsections (d) and (f).

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NRO will, nevertheless, continue to publish such a notice in broad generic terms as is its current practice.

(vi) Consistent with the legislative purpose of the Privacy Act of 1974, the NRO will grant access to nonexempt material in the records being maintained. Disclosure will be governed by NRO's Privacy Regulation, but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal or civil violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered; the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of the above nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated in this paragraph. The decisions to release information from these systems will be made on a case-by-case basis.

(i) NRO–21.

(1) *System name:* Personnel Security Files.

(2) *Exemptions:* (i) Investigatory material compiled for law enforcement purposes may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source.

(ii) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(iii) Therefore, portions of this system of records may be exempt pursuant to 5 U.S.C. 552a(k)(2) and/or (k)(5) from the following subsections of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H) and (I), and (f).

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

(4) *Reasons:* (i) From subsection (c)(3) because to grant access to the accounting for each disclosure as required by the Privacy Act, including the date, nature, and purpose of each disclosure and the identity of the recipient, could alert the subject to the existence of the investigation or prosecutable interest by the NRO or other agencies. This could seriously compromise case preparation by prematurely revealing its existence and nature; compromise or

interfere with witnesses or make witnesses reluctant to cooperate; and lead to suppression, alteration, or destruction of evidence.

(ii) From subsections (d)(1) through (d)(4), and (f) because providing access to records of a civil or administrative 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; enable individuals to conceal their wrongdoing or mislead the course of the investigation; 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) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because this system of records is compiled for law enforcement purposes and is exempt from the access provisions of subsections (d) and (f).

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NRO will, nevertheless, continue to publish such a notice in broad generic terms as is its current practice.

(vi) Consistent with the legislative purpose of the Privacy Act of 1974, the NRO will grant access to nonexempt material in the records being maintained. Disclosure will be governed by NRO's Privacy Regulation, but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered; the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of the above nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated above. The decisions to release information from these systems will be made on a case-by-case basis.

(j) QNRO–4.

(1) *System name:* Freedom of Information Act and Privacy Act Files.

(2) *Exemption:* During the processing of a Freedom of Information Act/Privacy Act request, exempt materials from other systems of records may in turn become part of the case record in this system. To the extent that copies of exempt records from those ''other'' systems of records are entered into this system, the NRO hereby claims the same exemptions for the records from those ''other'' systems that are entered into this system, as claimed for the original primary system of which they are a part.

(3) Authority: 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), (k)(3), (k)(4), (k)(5), (k)(6), and (k)(7).

(4) Records are only exempt from pertinent provisions of 5 U.S.C. 552a to the extent such provisions have been identified and an exemption claimed for the original record and the purposes underlying the exemption for the original record still pertain to the record which is now contained in this system of records. In general, the exemptions were claimed in order to protect properly classified information relating to national defense and foreign policy, to avoid interference during the conduct of criminal, civil, or administrative actions or investigations, to ensure protective services provided the President and others are not compromised, to

protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations, and to preserve the confidentiality and integrity of Federal evaluation materials. The exemption rule for the original records will identify the specific reasons why the records are exempt from specific provisions of 5 U.S.C. 552a.

(k) QNRO–27.

(1) *System name:* Legal Records.

(2) *Exemption:* Any portion of this system of records which falls within the provisions of 5 U.S.C. 552a(k)(2) and (k)(5) may be exempt from the following subsections of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f).

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

(4) *Reasons:* (i) From subsection (c)(3) because to grant access to the accounting for each disclosure as required by the Privacy Act, including the date, nature, and purpose of each disclosure and the identity of the recipient, could alert the subject to the existence of the investigation. This could seriously compromise case preparation by prematurely revealing its existence and nature; compromise or interfere with witnesses or make witnesses reluctant to cooperate; and lead to suppression, alteration, or destruction of evidence.

(ii) From subsections (d) and (f) because providing access to investigative records 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; enable individuals to conceal their wrongdoing or mislead the course of the investigation; 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) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because this system of records is compiled for investigative purposes and is exempt from the access provisions of subsections (d) and (f).

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants.

[65 FR 20372, Apr. 17, 2000, as amended at 66 FR 41783, Aug. 9, 2001; 66 FR 54926, Oct. 31, 2001; 67 FR 17616, Apr. 11, 2002; 74 FR 55784, Oct. 29, 2009]

PART 327—DEFENSE COMMISSARY AGENCY PRIVACY ACT PROGRAM

Sec.

AUTHORITY: Pub. L. 93–579, 88 Stat. 1896 (5 U.S.C. 522a).

SOURCE: 65 FR 39806, June 28, 2000, unless otherwise noted.

§ 327.1 Purpose.

This part implements the basic policies and procedures for the implementation of the Privacy Act of 1974, as amended (5 U.S.C. 552a); OMB Circular

A–130;[1] and 32 CFR part 310; and to promote uniformity in the DeCA Privacy Act Program.

§ 327.2 Applicability.

This part applies to Headquarters, Field Operating Activities (FOA), Regions, Zones, Central Distribution Centers (CDC), Commissaries of DeCA, and contractors during the performance of a contract with DeCA. All personnel are expected to comply with the procedures established herein.

§ 327.3 Responsibilities.

(a) *The Director, DeCA.* (1) Supervises the execution of the Privacy Act and this part within the DeCA, and serves as the DeCA Privacy Act Appeal Authority.

(2) Appoints:

(i) The Executive Director for Support as the DeCA Initial Denial Authority for the DeCA Privacy Act Program.

(ii) The Records Manager, Office of Safety, Security, and Administration as the DeCA Privacy Act Officer.

(b) *The Privacy Act Officer, DeCA.* (1) Establishes and manages the PA program for DeCA.

(2) Provides guidance, assistance and training.

(3) Controls and monitors all requests received and prepares documentation to the office of primary responsibility (OPR) for response.

(4) Prepares response to requester based on information provided by the OPR.

(5) Signs all response requests for releasable information to the requester after coordination through the General Counsel. Ensures that all denied requests for information are released by the DeCA Initial Denial Authority.

(6) Publishes instructions to contractors that:

(i) Provide DeCA Privacy program guidance to their personnel who solicit, award, or administer government contracts;

(ii) Inform prospective contractors of their responsibilities regarding the DeCA Privacy Program; and

(iii) Establish an internal system of contractor performance review to ensure compliance with DeCA's Privacy program.

(iv) Prepare and submit System Notices to the Defense Privacy Office for publication in the FEDERAL REGISTER.

(7) Maintain Privacy Case files and records of disclosure accounting.

(8) Submit the DeCa Annual Privacy Act Report (RCS: DD-DA&M(A)1379) to the Defense Privacy Office.

(c) *DeCA Directorates/Staff Offices.* (1) Provide response and the information requested to the PA Officer for release to the individual.

(2) In the event the information is to be denied release, the requested information and rationale for denial will be forwarded to the PA Officer for denial determination.

(d) *Regions.* Regional Directors will appoint a Regional PA Coordinator who will maintain suspense control of PA actions, prepare documentation to the OPR for response, forward the information to the DeCA PA Officer for release determination, and notify the requester that the response will be received from the DeCA PA Officer using the format in Appendix A to this part.

(e) *DeCA Field Operating Activities (FOAs).* (1) Upon receipt of a PA request that has not been received from the DeCA PA Officer, notify the DeCA PA Officer within 2 days.

(2) Collect all information available and forward to the DeCA PA Officer. If the requested information is not available, provide the DeCA PA Officer the rationale to respond to the requester.

(f) *Central Distribution Centers (CDCs) and Commissaries.* (1) Upon receipt of a PA request, not received from the Region Coordinator, notify the Region Coordinator within 2 days.

(2) Collect all information available and forward it to the Region Coordinator for submission to DeCA PA Officer. If requested information is not available, provide the Region Coordinator the rationale so they can prepare a response to the DeCA PA Officer. If the information is available but determined to be exempt, provide the Region Coordinator with the requested information and specific reasons why the request should be denied. The Region Coordinator will formalize a reply to

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

the DeCA PA Officer, forwarding requested information and reasons for denial. The DeCA PA Officer will prepare the response to the requester with coordination by the General Counsel and signature by the IDA.

§ 327.4 Definitions.

Access. The review of a record of 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.

Computer room. Any combination of electronic hardware and software integrated in a variety of forms (firmware, programmable software, hard wiring, or similar equipment) that permits the processing of textual data. The equipment contains device to receive information and other processors with various capabilities to manipulate the information, store and provide input.

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.

Federal Register system. Established by Congress to inform the public of interim, proposed, and final regulations or rulemaking documents having substantial impact on the public. In this case, DeCA directives have the same meaning as regulations or rulemaking documents. The secondary role of the Federal Register system is to publish notice documents of public interest.

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.''

Individual access. Access to information pertaining to the individual by the individual or his or her designated agent or legal guardian.

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.

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. The Privacy Act of 1974, as amended, (5 U.S.C. 552a).

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

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

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.

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, hard wiring, 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.

§ 327.5 Systems of records.

(a) *System of records.* To be subject to the provisions of this part, a ''system of records'' must:

(1) Consist of ''records'' that are retrieved by the name of an individual or some other personal identifier, and

(2) Be under the control of DeCA.

(b) *Retrieval practices.* 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 the control of DeCA. The records MUST BE, in fact, retrieved by name or other personal identifier to become a system of records for DeCA.

(c) *Relevance and necessity.* Only those records that contain personal information which is relevant and necessary to accomplish a purpose required by Federal statute or an Executive Order will be maintained by DeCA.

(d) *Authority to establish systems of records.* Director, DeCA has the authority to establish systems of records; however, each time a system of records is established, the Executive Order or Federal statute that authorizes maintaining the personal information must be identified.

(1) DeCA will not maintain any records describing how an individual exercises his or her rights guaranteed by the First Amendment of the U.S. Constitution.

(2) These 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.

(e) *System manager's evaluation.* Systems managers, along with the DeCA Privacy Officer, shall 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 will also occur when a system notice amendment or alteration is prepared. Consider the following:

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

(2) The specific impact on the purpose or mission of not collecting each category of information contained in the system.

(3) The possibility of meeting the informational requirements through use of information not individually identifiable or through other techniques, such as sampling.

(4) The length of time each item of personal information must be retained.

(5) The cost of maintaining the information.

(6) The necessity and relevancy of the information to the purpose for which it was collected.

(f) *Discontinued information requirements.* (1) When notification is received to stop collecting any category or item of personal information, the DeCA PA Officer will issue instructions to stop immediately and also excise this information from existing records, when feasible, and amend existing notice.

(2) Disposition of these records will be provided by the DeCA PA Officer in accordance with the DeCA Filing System.[3]

(g) *Government contractors.* (1) When DeCA contracts for the operation or maintenance of a system of records or a portion of a system of records by a contractor, the record system or the portion affected are considered to be maintained by DeCA and are subject to this part. DeCA is responsible for applying the requirements of this part to the contractor. The contractor and its employees are to be considered employees of DeCA for the purposes of the approved provisions of the Privacy Act during the performance of the contract. Consistent with the Defense Acquisition Regulation, contracts requiring the maintenance of a system of records or the portion of a system of records shall identify specifically the record system and the work to be performed and shall include in the solicitation and resulting contract such terms as are prescribed in the Defense Acquisition Regulation (DAR).[4]

(2) If the contractor must use or have access to individually identifiable information subject to this part to perform any part of a contract, and the information would have been collected and maintained by DeCA but for the award of the contract, these contractor activities are subject to this part.

(3) The restrictions in paragraphs (g)(1) and (g)(2) of this section do not apply to records:

(i) Established and maintained to assist in making internal contractor management decisions such as those maintained for use in managing the contract.

(ii) Those maintained as internal contractor employee records even when used in conjunction with providing goods and services to DeCA.

(4) Disclosure of records to contractors. Disclosure of personal records to a contractor for the use in the performance of any DeCA contract is considered a disclosure within the Department of Defense (DoD). The contractor is considered the agent of DeCA and is to be maintaining and receiving the records for DeCA.

(h) *Safeguarding personal information.* DeCA personnel will protect records in every system of records for confidentiality against alteration, unauthorized disclosure, embarrassment, or unfairness to any individual about when information is kept.

(1) Supervisor/Manager paper records maintained by DeCA personnel will be treated as 'For Official Use Only' (FOUO) documents and secured in locked file cabinets, desks or bookcases during non-duty hours. During normal working hours, these records will be out-of-sight if the working area is accessible to non-government personnel.

(2) Personnel records maintained by DeCA computer room or stand alone systems, will be safeguarded at all times. Printed computer reports containing personal data must carry the markings FOUO. Other media storing personal data such as tapes, reels, disk packs, etc., must be marked with labels which bear FOUO and properly safeguarded.

[3] Copies may be obtained: Defense Commissary Agency, ATTN: FOIA/Privacy Officer, 1300 E. Avenue, Fort Lee, VA 23801–1800.

[4] See footnote 3 to § 327.5.

(3) Adherence to paragraphs (h)(1) and (h)(2) of this section, fulfills the requirements of 32 CFR part 285.

(i) *Records disposal.* (1) DeCA records containing personal data will be shredded or torn to render the record unrecognizable or beyond reconstruction.

(2) The transfer of large quantities of DeCA records containing personal data to disposal activities is not considered a release of personal information under this part. The volume of such transfers makes it difficult or impossible to identify easily specific individual records. Care must be exercised to ensure that the bulk is maintained so as to prevent specific records from becoming readily identifiable. If the bulk is amintained, no special procedures are required. if the bulk cannot be maintained, dispose of the records by shredding or tearing to render the record unrecognizable or beyond reconstruction.

§ 327.6 Collecting personal information.

(a) *Collect directly from the individual.* To the greatest extent practicable, collect personal information directly from the individual to whom it pertains if the information may be used in making any determination about the rights, privileges, or benefits of the individual under any Federal program.

(b) *Collecting personal information from third parties.* It may not be practical to collect personal information directly from an individual in all cases. Some examples of this are:

(1) Verification of information through third party sources for security or employment suitability determinations;

(2) Seeking third party opinions such as supervisory comments as to job knowledge, duty performance, or other opinion-type evaluations;

(3) When obtaining the needed information directly from the individual is exceptionally difficult or may result in unreasonable costs; or

(4) Contacting a third party at the request of the individual to furnish certain information such as exact periods of employment, termination dates, copies of records, or similar information.

(c) *Collecting social security numbers (SSNs).* (1) It is unlawful for DeCA to deny an individual any right, benefit, or privilege provided by law because an individual refuses to provide his or her SSN. Executive Order 9397 authorizes solicitation and use of SSNs as numerical identifiers for individuals in most Federal record systems, however, it does not provide mandatory authority for soliciting.

(2) When an individual is requested to provide their SSN, they must be told:

(i) the uses that will be made of the SSN;

(ii) The statute, regulation or rule authorizing the solicitation of the SSN; and

(iii) Whether providingthe SSN is voluntary or mandatory.

(3) Once the SSN has been furnished for the purpose of establishing a record, the notification in paragraph (c)(2) of this section is not required if the individual is only requested to furnish or verify the SSNs for identification purposes in connection with the normal use of his or her records.

(d) *Privacy act statements.* When a DeCA individual is requested to furnish personal information about himself or herself for inclusion in a system of records, a Privacy Act Statement is required regardless of the medium used to collect the information, e.g., forms, personal interviews, telephonic interviews. The statement allows the individual to make a decision whether to provide the information requested. The statement will be concise, curent, and easily understood and must state whether providing the information is voluntary or mandatory. if furnishing the data is mandatory, a Federal statute, Executive Order, regulation or other lawful order must be cited. If the personal information solicited is not to be incorporated into a DeCA system of records, a PA statement is not required. This information obtained without the PA statement will not be incorporated into any DeCA systems of records.

(1) *The DeCA Privacy Act Statement will include:*

(i) The specific Federal statute or Executive Order that authorized collection of the requested information;

(ii) The principal purpose or purposes for which the information is to be used;

(iii) The routine uses that will be made of the information;

(iv) Whether providing the information is voluntary or mandatory; and

(v) The effects on the individual if he or she chooses not to provide the requested information.

(2) *Forms.* When DeCA uses forms to collect personal information, placement of the Privacy Act advisory statement should be in the following order of preference:

(i) Below the title of the form and positioned so the individual will be advised of the requested information,

(ii) Within the body of the form with a notation of its location below the title of the form,

(iii) On the reverse of the form with a notation of its location below the title of the form,

(iv) Attached to the form as a tear-off sheet, or

(v) Issued as a separate supplement to the form.

(3) *Forms issued by non-DoD Activities.* Ensure that the statement prepared by the originating agency on their forms is adequate for the purpose for which DeCA will use the form. If the statement is inadequate, DeCA will prepare a new statement before using the form. Forms issued by other agencies not subject to the Privacy Act but its use requires DeCA to collect personal data, a Privacy Act Statement will be added.

§ 327.7 Access by individuals.

(a) *Individual access to personal information.* Release of personal information to individuals whose records are maintained in a systems of records under this part is not considered public release of information. DeCA will release to the individuals all of the personal information, except to the extent the information is contained in an exempt system of records.

(1) *Requests for access.* (i) Individuals in DeCA Headquarters and FOAs will address requests for access to their personal information to the DeCA Privacy Act Officers. Individuals in Regions, CDCs, and commissaries, will address requests to their respective Region Privacy Act Coordinator. The individual is not required to explain or justify why access is being sought.

(ii) If an individual wishes to be accompanied by a third party when seeking access to his or her records or to have the records released directly to the third party, a signed access authorization granting the third party access is required.

(iii) A DeCA individual will not be denied access to his or her records because he or she refuses to provide his or her SSN unless the SSN is the only way retrieval can be made.

(2) *Granting access.* (i) If the record is not part of an exempt system, DeCA personnel will be granted access to the original record or an exact copy of the original record without any changes or deletions. Medical records will be disclosed to the individual to whom they pertain unless an individual fails to comply with the established requirements. This includes refusing to name a physician to receive medical records when required, refusing to pay fees, or when a judgment is made that access to such records may have an adverse effect on the mental or physical health of the individual. Where an adverse effect may result, a release will be made in consultation with a physician.

(ii) DeCA personnel may be denied access to information compiled in reasonable anticipation of a civil action or proceeding. The term ''civil proceeding'' is intended to include quasi-judicial and pretrial judicial proceedings. Information prepared in conjunction with the quasi-judicial, pretrial and trial proceedings to include those prepared by DeCA legal and non-legal officials of the possible consequences of a given course of action are protected from access.

(iii) Requests by DeCA personnel for access to investigatory records pertaining to themselves, compiled for law enforcement purposes, are processed under this part and that of 32 CFR part 310. Those requests by DeCA personnel for investigatory records pertaining to themselves that are in records systems exempt from access provisions shall be processed under this part or 32 CFR part 285, depending upon which provides the greatest degree of access.

(3) *Non agency records.* (i) Uncirculated personal notes and records that are not given or circulated to any person or organization (example, personal

telephone list) that are kept or discarded at the author's discretion and over which DeCA exercises no direct control, are not considered DeCA records. However, if personnel are officially directed or encouraged, either in writing or orally, to maintain such records, they may become ''agency records'' and may be subject to this part.

(ii) Personal uncirculate handwritten notes of team leaders, office supervisors, or military supervisory personnel concerning subordinates are not a system of records within the meaning of this part. Such notes are an extension of the individual's memory. These notes, however, must be maintained and discarded at the discretion of the individual supervisor and not circulated to others. Any established requirement to maintain such notes (written or oral directives, regulation or command policy) make these notes ''AGENCY RECORDS.'' If the notes are circulated, they must be made a part of the system of records. Any action that gives personal notes the appearance of official agency records is prohibited unless they have been incorporated into a DeCA system of records.

(b) *Relationship between the Privacy Act and the Freedom of Information Act (FOIA).* (1) Requests from DeCA individuals for access to a record pertaining to themselves made under the FOIA are processed under the provisions of this part, 32 CFR part 310 and DeCA Directive 30–12, Freedom of Information Act (FOIA) Program.[5]

(2) Request from DeCA individuals or access to a record pertaining to themselves are processed under this part and 32 CFR part 310.

(3) Requests from DeCA individuals for access to records about themselves that cite both Acts or the DeCA implementing directives for both Acts are processed under this part except:

(i) When the access provisions of the FOIA provide a greater degree of access process under the FOIA, or

(ii) When access to the information sought is controlled by another Federal statute process access procedures under the controlling statute.

(4) Requests from DeCA individuals for access to information about themselves in a system of records that do not cite either Act or DeCA implementing directive are processed under the procedures established by this part.

(5) DeCA requesters will not be denied access to personal information concerning themselves that would be releasable to them under either Act because they fail to cite either Act or the wrong Act. The Act or procedures used in granting or denying access will be explained to requesters.,

(6) DeCA requesters should receive access to their records within 30 days.

(7) Records in all DeCA systems maintained in accordance with the Government-wide systems notices are in temporary custody of DeCA, and all requests or amend these records will be processed in accordance with this part.

(c) *Denial of individual access.* (1) A DeCA individual may be denied formal access to a record pertaining to him/her only if the record:

(i) Was compiled in reasonable anticipation of civil action.

(ii) Is in a system of records that has been exempt from access provisions of this part.

(iii) All systems of records maintained by the Defense Commissary Agency shall be exempt from the requirements of 5 U.S.C. 552a(d) pursuant to 5 U.S.C. 552a(k)(1) to the extent that the system contains any information properly classified under Executive Order 12958 and which is required by the Executive Order to be withheld 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 herein may contain items of information that have been properly classified.

(iv) Is contained in a system of records for which access may be denied under some other Federal statute.

(v) All systems of records maintained by the DeCA shall be exempt from the requirements of 5 U.S.C. 552a(d) pursuant to 5 U.S.C. 552a(k)(1) to the extent that the system contains any information properly classified under Executive Order 12958 and which is required by the Executive Order to be withheld

[5] See footnote 3 to § 327.5.

in the interest of national defense of 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 herein may contain items of information that have been properly classified.

(2) DeCA individuals will only be denied access to those portions of the records from which the denial of access serves some legitimate governmental purpose.

(3) Other reasons to refuse DeCA individuals are:

(i) The request is not described well enough to locate it within a reasonable amount of effort by the PA Officer or PA Coordinator; or

(ii) An individual fails to comply with the established requirements including refusing to name a physician to receive medical records when required or to pay fees.

(4) Only the DeCA IDA can deny access. This denial must be in writing and contain:

(i) The date of the denial, name, title of position, and signature of the DeCA Initial Denial Authority.

(ii) The specific reasons for the denial, including specific reference to the appropriate sections of the PA, other statutes, this part or the Code of Federal Regulations (CFR);

(iii) Information providing the right to appeal the denial through the DeCa appeal procedure within 60 days, and the title, position and address of the DeCA PA Appellate Authority.

(5) *DeCA Appeal Procedures.* The Director of DeCA, or the designee, will review any appeal by an individual from a denial of access to DeCA records. Formal written notification will be provided to the individual explaining whether the denial is sustained totally or in part. The DeCA PA Officer will:

(i) Assign a control number and process the appeal to the Director, DeCA or the designee appointed by the Director.

(ii) Provide formal written notification to the individual by the appeal authority explaining whether the denial is sustained totally or in part and the exact reasons for the denial to include provisions of the Act, other statute, this part or the CFR whichever the determination is based, or

(iii) Provide the individual access to the material if the appeal is granted.

(iv) Process all appeals within 30 days of receipt unless the appeal authority determines the review cannot be made within that period and provide notification to the individual the reasons for the delay and when an answer may be expected.

(d) *Amendment of records.* (1) DeCA employees are encouraged to review the personal information being maintained abut them periodically. An individual may request amendment of any record contained in a system of records unless the system of records has been exempt specifically from the amendment procedures by the Director, DeCa. A request for amendment must include:

(i) A description of the item or items to be amended.

(ii) The specific reason for the amendment.

(iii) The type of amendment action such as deletion, correction or addition.

(iv) Copies of evidence supporting the request.

(v) DeCA employees may be required to provide identification to make sure that they are indeed seeking to amend a record pertaining to themselves.

(2) The amendment process is not intended to permit the alteration of evidence presented in the course of judicial or quasi-judicial proceedings. Amendments to these records are made through specific procedures established for the amendment of these records.

(i) Written notification will be provided to the requester within 10 working days of its receipt by the DeCA PA Officer. No notification will be provided to the requester if the action completed within the 10 days. Only under exceptional circumstances will more than 30 days be required to reach the decision to amend a request. If the decision is to grant all or in part of the request for amendment, the record will be amended and the requester informed and all other offices/personnel known to be keeping the information.

(ii) If the request for amendment is denied in whole or in part, The PA Officer will notify the individual in writing and provide the specific reasons and the procedures for appealing the decision.

(iii) All appeals are to be processed within 30 days. If additional time is required, the requester will be informed and provided when a final decision may be expected.

(e) *Fee assessments.* (1) DeCA personnel will only be charged the direct cost of copying and reproduction, computed using the appropriate portions of the fee schedule in DeCA Directive 30–12.[6] Normally, fees are waived automatically if the direct costs of a given request are less than $30. This fee waiver provision does not apply when a waiver has been granted to the individual before, and later requests appear to be an extension or duplication of that original request. Decisions to waive or reduce fees that exceed the automatic waiver threshold will be made on a case-by-case basis. Fees may not be charged when:

(i) Copying is performed for the convenience of the Government or is the only means to make the record available for the individual.

(ii) No reading room is available for the individual to review the record or a copy is made to keep the original in DeCA files.

(iii) The information may be obtained without charge under any other regulation, directive, or statute.

(2) No fees will be collected for search, retrieval, and review of records to determine releasability, copying of records when the individual has not requested a copy, transportation of records and personnel, or normal postage.

§ 327.8 Disclosure of personal information to other agencies and third parties.

(a) *Disclosures and nonconsensual disclosures.* (1) All requests made by DeCA individuals for personal information about other individuals (third parties) will be processed under DeCA Directive 30–12[7] except when the third party personal information is contained in the Privacy record of the individual making the request.

(2) For the purposes of disclosure and disclosure accounting, the Department of Defense is considered a single agency.

(3) Personal information from DeCA systems of records will not be disclosed outside the DoD unless:

(i) The record has been requested by the individual to whom it pertains,

(ii) Written consent has been given by the individual to whom the record pertains for release to the requesting agency, activity, or individual, or

(iii) The release is pursuant to one of the specific nonconsensual purposes set forth in the Act.

(4) Records may be disclosed without the consent of a DeCA individual to any DoD official who has need for the record in the performance of their assigned duties. Rank, position, or title alone does not authorize this access. An official need for this information must exist.

(5) DeCA records must be disclosed if their release is required by 32 CFR part 285, which is implemented by DeCA Directive 30–12.[8] 32 CFR part 285 requires that records be made available to the public unless exempt from disclosure under the FOIA.

(b) *Normally releasable information.* Personal information that is normally releasable without the consent of a DeCA individual that does not imply a clearly unwarranted invasion of personal privacy:

(1) Civilian employees:

(i) Name,

(ii) Present and past position titles,

(iii) Present and past grades,

(iv) Present and past salaries,

(v) Present and past duty stations,

(vi) Office or duty telephone numbers,

(2) Military members:

(i) Full name,

(ii) Rank,

(iii) Date of rank,

(iv) Gross salary,

(v) Past duty assignments,

(vi) Present duty assignments,

(vii) Future assignments that are officially established,

(viii) Office or duty telephone numbers,

(ix) Source of commission,

(x) Promotion sequence number,

(xi) Awards and decorations,

[6] See footnote 3 to § 327.5.

[7] See footnote 3 to § 327.5.

[8] See footnote 3 to § 327.5.

(xii) Attendance at professional military schools,

(xiii) Duty status at any given time.

(3) All disclosures of personal information on civilian employees shall be made in accordance with the Office of Personnel Management (OPM) and all disclosures of personal information on military members shall be made in accordance with the standards established by 32 CFR part 285.

(4) The release of DeCA employees' home addresses and home telephone numbers is considered a clearly unwarranted invasion of personal privacy and is prohibited; however, these may be released without prior consent of the employee if:

(i) The employee has indicated previously that he or she consents to their release,

(ii) The releasing official was requested to release the information under the provisions of 32 CFR part 285.

(5) Before listing home addresses and home telephone numbers in any DeCA telephone directory, give the individuals the opportunity to refuse such a listing.

(c) *Disclosures for established routine uses.* (1) Records may be disclosed outside of DeCA without consent of the individual to whom they pertain for an established routine use.

(2) A routine use shall:

(i) Be compatible with the purpose for which the record was collected;

(ii) Indicate to whom the record may be released;

(iii) Indicate the uses to which the information may be put by the receiving agency; and

(iv) Have been published previously in the FEDERAL REGISTER.

(3) A routine use will be established for each user of the information outside DeCA who need official access to the records. This use may be discontinued or amended without the consent of the individual/s involved. Any routine use that is new or changed is published in the FEDERAL REGISTER 30 days before actually disclosing the record. In addition to routine uses established by DeCA individual system notices, blanket routine uses have been established. See Appendix C to this part.

(d) *Disclosure without consent.* DeCA records may be disclosed without the consent of the individual to whom they pertain to another agency within or under the control of the U.S. for a civil or criminal law enforcement activity if:

(1) The civil or criminal law enforcement activity is authorized by law (Federal, State, or local); and

(2) The head of the agency or instrumentality (or designee) has made a written request to the Component specifying the particular record or portion desired and the law enforcement activity for which it is sought.

(3) Blanket requests for any and all records pertaining to an individual shall not be honored. The requesting agency or instrumentality must specify each record or portion desired and how each relates to the authorized law enforcement activity.

(4) This disclosure provision applies when the law enforcement agency or instrumentality request the record, If the DoD Component discloses a record outside the DoD for law enforcement purposes without the individual's consent and without an adequate written request, the disclosure must be pursuant to an established routine use, such as the blanket routine use for law enforcement.

(e) *Disclosures to the public from health care records.* (1) The following general information may be released to the news media or public concerning a DeCA employee treated or hospitalized in DoD medical facilities and non-Federal facilities for whom the cost of the care is paid by DoD:

(i) Personal information concerning the patient that is provided in § 327.8 and under provisions of 32 CFR part 285.

(ii) The medical condition such as the date of admission or disposition and the present medical assessment of the individual's condition in the following terms if the medical doctor has volunteered the information:

(A) The individual's condition is presently (stable) (good) (fair) (serious) or (critical), and

(B) Whether the patient is conscious, semi-conscious or unconscious.

(2) Detailed medical and other personal information may be released on a DeCA employee only if the employee has given consent to the release. If the

employee is not conscious or competent, no personal information, except that required by 32 CFR part 285, will be released until there has been enough improvement in the patient's condition for them to give informed consent.

(3) Any item of personal information may be released on a DeCA patient if the patient has given consent to its release.

(4) This part does not limit the disclosure of personal medical information for other government agencies' use in determining eligibility for special assistance or other benefits provided disclosure in pursuant to a routine use.

APPENDIX A TO PART 327—SAMPLE DECA RESPONSE LETTER

Mrs. Floria Employee
551 Florida Avenue
Oakland, CA 94618

Dear Mrs. Employee: This responds to your Privacy Act request dated (enter date of request), in which you requested (describe requested records).

Your request has been referred to our headquarters for further processing. They will respond directly to you. Any questions concerning your request may be made telephonically (enter Privacy Officer's telephone number) or in writing to the following address:

Defense Commissary Agency, Safety, Security, and Administration, Attention: FOIA/PA Officer, Fort Lee, VA 23801–1800.

I trust this information is responsive to your needs.

(Signature block)

APPENDIX B TO PART 327—INTERNAL MANAGEMENT CONTROL REVIEW CHECKLIST

(a) *Task:* Personnel and/or Organization Management.

(b) *Subtask:* Privacy Act (PA) Program.

(c) *Organization:*

(d) *Action officer:*

(e) *Reviewer:*

(f) *Date completed:*

(g) *Assessable unit:* The assessable units are HQ, DeCA, Regions, Central Distribution Centers, Field Operating Activities, and commissaries. Each test question is annotated to indicate which organization(s) is (are) responsible for responding to the question(s). Assessable unit managers responsible for completing this checklist are shown in the DeCA, MCP, DeCA Directive 70–2.[1]

(h) *Event cycle 1:* Establish and implement a Privacy Act Program.

(1) Risk: If prescribed policies, procedures and responsibilities of the Privacy Act Program are not adhered to, sensitive private information on individuals can be given out to individuals.

(2) Control Objectives: The prescribed policies, procedures and responsibilities contained in 5 U.S.C. 552a are followed to protect individual privacy and information release.

(3) Control Techniques: 32 CFR part 310 and DeCA Directive 30–13,[2] Privacy Act Program.

(i) Ensure that a PA program is established and implemented.

(ii) Appoint an individual with PA responsibilities and ensure the designation of appropriate staff to assist.

(4) Test Questions: Explain rationale for YES responses or provide cross-references where rationale can be found. For NO responses, cross-reference to where corrective action plans can be found. If response is NA, explain rationale.

(i) Is a PA program established and implemented in DeCA to encompass procedures for subordinate activities? (DeCA HQ/SA, Region IM). Response: Yes / No / NA. Remarks:

(ii) Is an individual appointed PA responsibilities? (DeCA HQ/SA, Region IM). Response: Yes / No / NA. Remarks:

(iii) Are the current names and office telephone numbers furnished OSD, Private Act Office of the PA Officer and the IDA? (DeCA HQ/SA). Response: Yes / No / NA. Remarks:

(iv) Is the annual PA report prepared and forwarded to OSD, Defense Privacy Office? (DeCA HQ/SA). Response: Yes / No / NA. Remarks:

(v) Is PA awareness training/orientation provided? Is in-depth training provided for personnel involved in the establishment, development, custody, maintenance and use of a system of records? (DeCA HQ/SA, Region). Response: Yes / No / NA. Remarks:

(vi) Is the PA Officer consulted by information systems developers for privacy requirements which need to be included as part of the life cycle management of information consideration in information systems design? (DeCA HQ/SA, Region). Response: Yes / No / NA. Remarks:

(vii) Is each system of records maintained by DeCA supported by a Privacy Act System Notice and has the systems notice been published in the FEDERAL REGISTER? (DeCA HQ/SA). Response: Yes / No / NA. Remarks:

(i) *Event cycle 2:* Processing PA Requests.

[1] Copies may be obtained: Defense Commissary Agency, ATTN: FOIA/Privacy Officer, 1300 E. Avenue, Fort Lee, VA 23801–1800.

[2] See footnote 1 to this Appendix B.

(1) Risk: Failure to process PA requests correctly could result in privacy information being released which subjects the Department of Defense, DeCA or individuals to criminal penalties.

(2) Control Objective: PA requests are processed correctly.

(3) Control Technique:

(i) Ensure PA requests are logged into a formal control system.

(ii) Ensure PA requests are answered promptly and correctly.

(iii) Ensure DeCA records are only withheld when they fall under the general and specific exemptions of 5 U.S.C. 552a and one or more of the nine exemptions under DeCA Directive 30–12,[3] Freedom of Information Act (FOIA) Program.

(iv) Ensure all requests are coordinated through the General Counsel.

(v) Ensure all requests are denied by the DeCA IDA.

(vi) Ensure all appeals are forwarded to the Director DeCA or his designee.

(4) Test Questions:

(i) Are PA requests logged into a formal control system? (DeCA HQ/SA, Region IM). Response: Yes / No / NA. Remarks:

(ii) Are individual requests for access acknowledged within 10 working days after receipt? (DeCA HQ/SA, Region IM). Response: Yes / No / NA. Remarks:

(iii) when more than 10 working days are required to respond to a PA request, is the requester informed, explaining the circumstances for the delay and provided an approximate date for completion? (DeCA HQ/SA, Region IM). Response: Yes / No / NA. Remarks:

(iv) Are DeCA records withheld only when they fall under one or more of the general or specific exemptions of the PA or one or more of the nine exemptions of the FOIA? (DeCA HQ/SA, Region IM). Response: Yes / No / NA. Remarks:

(v) Do denial letters contain the name and title or position of the official who made the determination, cite the exemption(s) on which the denial is based and advise the PA requester of their right to appeal the denial to the Director DeCA or designee? (DeCA HQ/SA). Response: Yes / No / NA. Remarks:

(vi) Are PA requests denied only by the HQ DeCA IDA? (All). Response: Yes / No / NA. Remarks:

(vii) Is coordination met with the General Counsel prior to forwarding a PA request to the IDA? (DeCA HQ/SA). Response: Yes / No / NA. Remarks:

(j) *Event cycle 3:* Requesting PA Information.

(1) Risk: Obtaining personal information resulting in a violation of the PA.

(2) Control Objective: Establish a system before data collection and storage to ensure no violation of the privacy of individuals.

(3) Control Technique: Ensure Privacy Act Statement to obtain personal information is furnished to individuals before data collection.

(4) Test Questions:

(i) Are all forms used to collect information about individuals which will be part of a system of records staffed with the PA Officer for correctness of the Privacy Act Statement? (DeCA HQ/SA, Region). Response: Yes / No / NA. Remarks:

(ii) Are Privacy Statements prepared and issued for all forms, formats and questionnaires that are subject to the PA, coordinated with the DeCA forms manager? (DeCA HQ/SA, Region). Response: Yes / No / NA. Remarks:

(iii) Do Privacy Act Statements furnished to individuals provide the following:

(A) The authority for the request.

(B) The principal purpose for which the information will be used.

(C) Any routine uses.

(D) The consequences of failing to provide the requested information. Yes / No / NA. Remarks:

(k) *Event cycle 4:* Records Maintenance.

(1) Risk: Unprotected records allowing individuals without a need to know access to privacy information.

(2) Control Objective: PA records are properly maintained throughout their life cycle.

(3) Control Technique: Ensure the prescribed policies and procedures are followed during the life cycle of information.

(4) Test Questions:

(i) Are file cabinets/containers that house PA records locked at all times to prevent unauthorized access? (All). Response: Yes / No / NA. Remarks:

(ii) Are personnel with job requirement (need to know) only allowed access to PA information? (All). Response: Yes / No / NA. Remarks:

(iii) Are privacy act records treated as unclassified records and designated 'For Official Use Only'? (All). Response: Yes / No / NA. Remarks:

(iv) Are computer printouts that contain privacy act information as well as disks, tapes and other media marked 'For Official Use Only'? (All). Response: Yes / No / NA. Remarks:

(v) Is a Systems Manager appointed for each automated/manual PA systems of records? (DeCA HQ/SA, Region). Response: Yes / No / NA. Remarks:

(vi) Are PA records maintained and disposed of in accordance with DeCA Directive 30–2,[4] The Defense Commissary Agency Filing System? (All). Response: Yes / No / NA. Remarks:

[3] See footnote 1 to this Appendix B.

[4] See footnote 2 to this Appendix B.

(1) I attest that the above listed internal controls provide reasonable assurance that DeCA resources are adequately safeguarded. I am satisfied that if the above controls are fully operational, the internal controls for this sub-task throughout DeCA are adequate.

Safety, Security and Administration.

FUNCTIONAL PROPONENT.

I have reviewed this sub-task within my organization and have supplemented the prescribed internal control review checklist when warranted by unique environmental circumstances. The controls prescribed in this checklist, as amended, are in place and operational for my organization (except for the weaknesses described in the attached plan, which includes schedules for correcting the weaknesses).

ASSESSABLE UNIT MANAGER (Signature).

APPENDIX C TO PART 327—DECA BLANKET ROUTINE USES

(a) *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, 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.

(b) *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.

(c) *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.

(d) *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.

(e) *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.

(f) *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.

(g) *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.

(h) *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.

(i) *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.

(j) *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.

(k) *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.

(l) *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.

(m) *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.

(n) *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.

PART 329—NATIONAL GUARD BUREAU PRIVACY PROGRAM

Sec.

AUTHORITY: Pub. L. 93–579, 88 Stat. 1986 (5 U.S.C. 552a).

SOURCE: 79 FR 6809, Feb. 5, 2014, unless otherwise noted.

§ 329.1 Purpose.

This part implements the policies and procedures outlined in 5 U.S.C. 552a, Office of Management and Budget (OMB) Circular No. A–130, and 32 CFR part 310. This part provides the responsibilities, guidance, and procedures for the National Guard Bureau (NGB) to comply with Federal and DoD Privacy requirements.

§ 329.2 Applicability.

(a) This part applies to the NGB and the records under control of the Chief, NGB, as defined by DoD Directive (DoDD) 5105.77, entitled ''National Guard Bureau.'' (Available at *http://www.dtic.mil/whs/directives/corres/pdf/510577p.pdf*)

(b) This rule will cover the privacy policies and procedures associated with records created and under the control of the Chief, NGB that are not otherwise covered by existing DoD, Air Force, or Army rules.

§ 329.3 Definitions.

All terms used in this part which are defined in 5 U.S.C. 552a shall have the same meaning herein.

Access. Allowing individuals to review or receive copies of their records.

Accuracy. Within sufficient tolerance for error to assure the quality of the record in terms of its use in making a determination.

Agency. Any Executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the [federal] Government (including the Executive Office of the President), or any independent regulatory agency (as defined by 5 U.S.C. 552a).

Amendment. The process of adding, deleting, or changing information in a System of Records (SOR) to make the data accurate, relevant, timely, and/or complete.

Appellate authority. The individual with authority to deny requests for access or amendment of records under 5 U.S.C. 552a.

Breach. A loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where a person other than authorized users (with an official need to know), and for an other than authorized purpose has access or potential access to personally identifiable information, whether physical or electronic. A breach can include identifiable information in any form. (As defined by DoD Director of Administration and Management Memo, 5 Jun 2009 entitled ''Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII).'') (Available at *http://www.dod.mil/pubs/foi/privacy/docs/DA__M6__5__2009Responding__toBreach__of__PII.pdf*)

Chief, National Guard Bureau (CNGB). A principal advisor to the Secretary of Defense, through the Chairman of the Joint Chiefs of Staff, on matters involving non-federalized National Guard forces and on other matters as determined by the Secretary of Defense; and the principal adviser to the Secretary of the Army and the Chief of Staff of the Army, and to the Secretary of the Air Force and the Chief of Staff of the Air Force, on matters relating to the National Guard, the Army National Guard of the United States, and the Air National Guard of the United States. The CNGB also represents the National Guard on the Joint Chiefs of Staff.

Completeness. All elements necessary for making a determination are present before such determination is made.

Computer matching program. A program that matches the personal records in computerized database of two or more Federal agencies.

Denial authority. The individual with authority to deny requests for access or amendment of records under 5 U.S.C. 552a.

Determination. Any decision affecting an individual which, in whole or in part, is based on information contained in the record and which is made by any person or agency.

Directorate/Division. The terms directorate and division are used to refer to suborganizations within the NGB. The Joint Staff and Air Guard Readiness Center uses the term ''Directorate'' to refer to their suborganizations and the Army Guard Readiness Center uses the term ''Division'' to refer to their suborganizations.

Disclosure. Giving information from a system, by any means, to anyone other than the record subject.

Disclosure accounting. A record of all disclosures made from a SOR, except for disclosures made to Department of Defense personnel for use in performance of their official duties or disclosures made as required by 5 U.S.C. 552.

Federal Register (FR). A daily publication of notices and rules issued by Federal Agencies and the President printed on a daily Federal workday.

Individual. A citizen of the United States or an alien lawfully admitted for permanent residence. (As defined by 5 U.S.C. 552a)

Maintain. Maintain, collect, use or disseminate. (As defined by 5 U.S.C. 552a)

Memorandum of Agreement. A written understanding (agreement) between parties to cooperatively work together on an agreed upon project or meet an agreed objective.

Memorandum of Understanding. A written agreement between parties describing a bilateral or multilateral agreement between parties.

Necessary. A threshold of need for an element of information greater than mere relevance and utility.

Personal information. Information about an individual other than items of public record.

Personally Identifiable Information (PII). Personal information. Information about an individual that identifies, links, relates, or is unique to, or describes him or her. Information which can be used to distinguish or trace an individual's identity which is linked or linkable to a specified individual.

Privacy Act (5 U.S.C. 552a) Request. An oral (in person) or written request by an individual to access his or her records in a SOR.

Privacy Act (5 U.S.C. 552a) Statement (PAS). A statement given to an individual when soliciting personal information that will be maintained in a

SOR that advises them of the authority to collect information, the principal purpose(s) that the information will be used for, the routine uses on how the information will be disclosed outside of the agency, and whether it is mandatory or voluntary to provide the information and any consequences for not providing the information.

Privacy Impact Assessment (PIA). A written assessment of an information system that addresses the information to be collected, the purpose and intended use; with whom the information will be shared; notice or opportunities for consent to individuals; how the information will be secured; and whether a new SOR is being created under 5 U.S.C. 552a. Privacy Impact Assessments are required for all information systems and electronic collections that collect, maintain, use, or disseminate personally identifiable information about members of the public (this includes contractors and family members), under Public Law 107–347, Section 208 of the E-Government Act of 2002. DoD Regulation 5400.16–R, entitled ''Department of Defense Privacy Impact Assessment (PIA)'' (Available at *http://www.dtic.mil/whs/directives/corres/pdf/540016p.pdf*), provides additional requirements for PIAs, including a requirement to write a PIA on any information systems or electronic collection of PII on Federal personnel.

Protected Health Information (PHI). Any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

Record. Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, the individual's education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph (As defined by 5 U.S.C. 552a).

Relevance. Limitation to only those elements of information that clearly bear of the determination(s) for which the records are intended.

Routine use. The disclosure of a record outside the DoD for a use that is compatible with the purpose for which the information was collected and maintained by the DoD. The routine use must be included in the published system notice for the SOR involved. The DoD Blanket Routine Uses, found in 32 CFR part 310, Appendix C are applicable to all SORNs published by DoD.

System Manager. The official who is responsible for managing a SOR, including policies and procedures to operate and safeguard it. Local System Managers operate record systems or are responsible for the records that are maintained in decentralized locations but are covered by a SORN published by another DoD activity or a Government-Wide SORN.

System of Records (SOR). A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

System of Records Notice (SORN). The official public notice published in the FR of the existence and content of the SOR. As required by 5 U.S.C. 552a and 32 CFR part 310, appendix E. The notice shall include:

(1) System ID.

(2) The name and location of the system.

(3) The categories of individuals on whom records are maintained in the system.

(4) The categories of records maintained in the system.

(5) Each routine use of the records contained in the system, including the categories of users and the purpose of such use.

(6) The policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records.

(7) The title and business address of the agency official who is responsible for the SOR.

(8) The agency procedures whereby an individual can be notified at his request if the SOR contains a record pertaining to him.

(9) The agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in

the SOR, and how he can contest its contents.

(10) The categories of sources of records in the system.

(11) Exemptions claimed for the system.

Timeliness. Sufficiently current to ensure that any determination based on the record will be accurate and fair.

§ 329.4 Policy.

In accordance with 32 CFR part 310, it is NGB's policy that:

(a) Personal information contained in any SOR maintained by any NGB organization will be safeguarded to the extent authorized by 5 U.S.C. 552a, Appendix I of Office of Management and Budget Circular No. A–130, and any other applicable legal requirements.

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

(c) NGB will collect personal information directly from the individuals to whom it pertains to the greatest extent possible and will provide individuals a PAS at the time of collection when the information being collected will be filed and/or retrieved by the subject's name or other unique identifier. The PAS will contain the following elements, as required by 5 U.S.C. 552a:

(1) The statutory authority or Executive Order that allows for the solicitation,

(2) The intended use/purpose that will be made of the information collected,

(3) The routine uses that may be made of the information collected; and

(4) Whether it is mandatory or voluntary for the individual to disclose the requested information and the nonpunitive effects on the individual for not providing all or any part of the requested information. Collection can only be mandatory if the statutory authority or Executive Order cited provides a penalty for not providing the information.

(d) NGB offices maintaining records and information about individuals will ensure that such data is protected from unauthorized access, use, dissemination, disclosure, alteration, and/or destruction. Offices will establish safeguards to ensure the security of personal information is protected from threats or hazards that might result in substantial harm, embarrassment, inconvenience, or unfairness to the individual using guidelines found in 32 CFR part 310, subpart B, 32 CFR part 310, appendix A, and DoD Manual (DoDM) 5200.01, Volume 4, entitled ''DoD Information Security Program: Controlled Unclassified Information (CUI).''

(Available at *http://www.dtic.mil/whs/directives/corres/pdf/520001__vol4.pdf*)

(e) NGB offices shall permit individuals to access and have a copy of all or any portion of records about them, unless an exemption for the system has been properly established (see 5 U.S.C. 552a, 32 CFR part 310, subparts D and F, and § 329.7 of this part). Individuals requesting access to their record will also receive concurrent consideration under 5 U.S.C. 552 and 32 CFR part 286.

(f) NGB offices will permit individuals an opportunity to request that records about them be corrected or amended (see 5 U.S.C. 552a, 32 CFR part 310, subpart D, and § 329.6 of this part).

(g) Any records about individuals that are maintained by the NGB will be maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual before making any determination about the individual or before making the record available to any recipient pursuant to a routine use.

(h) NGB will keep no record that describes how individuals exercise their rights guaranteed by the First Amendment, 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.

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

(j) NGB will assist individuals in determining what records pertaining to them are being collected, maintained, used, or disseminated.

(k) NGB offices and personnel, including contractors, maintaining and having access to records and information about individuals will manage them and conduct themselves so as to

avoid the civil liability and criminal penalties provided for under 5 U.S.C. 552a.

§ 329.5 Responsibilities.

(a) *Chief of the National Guard Bureau (CNGB).* The CNGB, under the authority, direction, and control of the Secretary of Defense (SecDef), approves and establishes overall policy, direction, and guidance for the NGB privacy program and promulgates privacy policy for the non-Federalized National Guard.

(b) *NGB Chief Counsel.* The NGB Chief Counsel, under the authority, direction, and control of the CNGB, shall:

(1) Serve as the National Guard Component Senior Official for Privacy (CSOP) pursuant to part 32 CFR part 310, subpart A.

(2) Direct and administer the Privacy Program for the NGB as well as the National Guard of the States, Territories, and the District of Columbia as it pertains to the maintenance of records protected by 5 U.S.C. 552a, other Federal laws on privacy, and OMB and DoD Privacy policies.

(3) Ensure implementation of and compliance with standards and procedures established by 5 U.S.C. 552a, OMB A–130, 32 CFR part 310, and this part.

(4) Serve as the appellate authority on denials of access or amendment.

(5) Direct the implementation all aspects of 5 U.S.C. 552a, OMB A–130, 32 CFR part 310, this part, and other Federal laws on privacy, and OMB and DoD Privacy policies.

(c) *Chief of the Office of Information and Privacy (OIP).* The Chief of the OIP, under the authority, direction, and control of the NGB Chief Counsel, shall:

(1) Oversee the National Guard's compliance with 5 U.S.C. 552a, OMB A–130, 32 CFR part 310, this part, and other Federal laws on privacy, and OMB and DoD Privacy policies.

(2) Issue policy and guidance as it relates to 5 U.S.C. 552a and other Federal and DoD Privacy requirements.

(3) Collect, consolidate, and submit Privacy reports to the Defense Privacy and Civil Liberties Office (DPCLO), or the respective service (Air Force or Army) that the reporting of information pertains to. This includes, but is not limited to:

(i) Personally Identifiable Information (PII) Breach Reports required by 32 CFR part 310, subpart B,

(ii) Quarterly Training Reports, SORN Reviews, and Privacy Complaints; and,

(iii) Reports pursuant Public Law 17–347.

(4) Submit all approved SORNs to the DPCLO or the respective service that has the statutory authority to publish the SORN for publication in the FR.

(5) Refer inquiries about access, amendments of records, and general and specific exemptions listed in a SORN to the appropriate System Manager.

(6) Review all instructions, directives, publications, policies, Memorandums of Agreement (MOA), Memorandums of Understanding (MOU), data sharing agreements, data transfer agreements, data use agreements, surveys (including web-based or electronic), and forms that involve or discuss the collection, retention, access, use, sharing, or maintenance of PII are to ensure compliance with this part.

(7) Make training resources available to NGB personnel, including contractors, regarding 5 U.S.C. 552a, OMB A–130, 32 CFR part 310, compliance with this part, and other Federal and DoD Privacy requirements.

(d) *Chief of Administrative Law.* The Chief of Administrative Law shall serve as the initial denial authority (IDA) to deny official requests for access or amendment to an individual's record pursuant to a published NGB SORN under 5 U.S.C. 552a or amendments to such records.

(e) *Chief of Litigation and Employment Law.* The Chief of Litigation and Employment Law will notify the Chief of the OIP of any complaint citing 5 U.S.C. 552a is filed in a U.S. District Court against the NGB, or any employee of NGB using the procedures outlined in § 329.6 of this part.

(f) *NGB Comptroller/Director of Administration and Management (DA&M).* The NGB Comptroller/DA&M shall ensure appropriate Federal Acquisition Regulation (FAR) (Available at *https://www.acquisition.gov/far/*) and Defense

Federal Acquisition Regulation Supplement (DFARS) (Available at *http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html*) clauses (FAR Subpart 24.1 related to 5 U.S.C. 552a and FAR subpart 24.2 related to 5 U.S.C. 552, as well as DFARS clauses 52.224–1 and/or 52.224–2) are included in all contracts that provide for contractor personnel to have access or maintain records, including records in information systems, that are covered by 5 U.S.C. 552a or that contain PII.

(g) *NGB Directorates/Divisions.* All NGB directorates/divisions maintaining records containing PII or that have personnel that have access to PII shall:

(1) Ensure that a SORN is published in the FR before collection of any information subject to 5 U.S.C. 552a is scheduled to begin.

(2) Ensure System Managers comply with all responsibilities outlined in paragraph (h) of this section. This includes referring any proposed denials of access or amendment under 5 U.S.C. 552a to the Chief of the OIP within 10 working days.

(3) Evaluate Privacy requirements for information systems and electronic collection or maintenance of PII in the early stages of system acquisition/development. This includes completing a PIA in accordance with the requirements of Public Law 107–347, section 208 of the E-Government Act of 2002, and DoD 5400.16–R.

(4) Ensure personnel, including contractors, who have access to PII complete appropriate Privacy training as required by 5 U.S.C. 552a, 32 CFR part 310, subpart H, and Part II of DoD Policy ''Safeguarding Against and Responding to Breaches of PII'' (*http://www.dod.mil/pubs/foi/privacy/docs/DA__M6__5__2009Responding__toBreach__of__PII.pdf*) as follows:

(i) Orientation Training: Training that provides individuals with a basic understanding of the requirements of 5 U.S.C. 552a as it applies to the individual's job performance. The training is for all personnel, as appropriate, and should be a prerequisite to all other levels of training.

(ii) Specialized Training: Training that provides information as to the application of specific provisions of this part to specialized areas of job performance. Personnel of particular concern include, but are not limited to personnel specialists, finance officers, special investigators, paperwork managers, public affairs officials, information technology professionals, and any other personnel responsible for implementing or carrying out functions under this part.

(iii) Management Training: Training that provides managers and decision makers considerations that they should take into account when making management decisions regarding the Privacy program.

(iv) Privacy Act (5 U.S.C. 552a) SOR Training: All individuals who work with a Privacy Act (5 U.S.C. 552a) SOR are trained on the provisions of the 5 U.S.C. 552a SORN(s) they work with, 32 CFR part 310, and this part.

(5) Ensure all instructions, directives, publications, policies, MOAs, MOUs, data sharing agreements, data transfer agreements, data use agreements, surveys (including Web-based or electronic surveys), and forms that involve the collection, retention, use, access, sharing, or maintenance of PII are coordinated with the Chief of the OIP.

(6) Ensure that any suspected or confirmed breaches of PII, or potential breaches of PII, are immediately reported to the Chief of the OIP in accordance with NGB Memorandum 380–16/33–361. (Available at *http://www.nationalguard.mil/sitelinks/links/NGB%20Memorandum%20380-16%2033-361,%20PII%20Incident%20Response%20Handling.pdf*).

(7) Ensure policies and administrative processes within their directorates are evaluated to ensure compliance with the procedures in this part.

(h) *System Managers.* System Managers will:

(1) Report any changes to their existing SORN(s) to the Chief of the OIP for publishing in the FR at least 90 working days before the intended change to the system.

(2) Review their published SORN(s) on a biennial basis and submit updates to the Chief of the OIP as necessary.

(3) Ensure appropriate training is provided for all users, to include contractors, which have access to records

covered by their published system notice.

(4) Ensure safeguards are in place to protect all records containing PII (electronic, paper, etc.) from unauthorized access, use, disclosure, alteration, and/or destruction using guidelines found in 32 CFR part 310, subpart B, 32 CFR part 310, appendix A, and DoDM 5200.01, Volume 4.

(5) Assist in responding to any complaints and inquiries regarding the collection or maintenance of, or access to information covered by their published SORN(s).

(6) Process all 5 U.S.C. 552a requests for access and amendment, as outlined in §329.6 of this part.

(7) Maintain a record of disclosures for any records covered by a SORN using a method that complies with 32 CFR part 310, subpart E when disclosing records outside of the agency (DoD). Such disclosures will only be made when permitted by a Routine Use published in the SORN.

(i) As required by 5 U.S.C. 552a and 32 CFR part 310, subpart E, the disclosure accounting will be maintained for 5 years after the disclosure, or for the life of the record, whichever is longer. The record may be maintained with the record disclosed, or in a separate file within the office's official record keeping system.

(ii) Pursuant to 5 U.S.C. 552a and 32 CFR part 310, subpart E, the disclosure accounting will include the release date, a description of the information released, the reason for the release; and, the name and address of the recipient.

§329.6 Procedures.

(a) *Publication of notice in the FR.* (1) A SORN shall be published in the FR of any record system meeting the definition of a SOR, as defined by 5 U.S.C. 552a.

(2) System Managers shall submit notices for new or revised SORNs through their Director to the Chief of the OIP for review at least 90 working days prior to implementation.

(3) The Chief of the OIP shall forward complete SORNs to the Defense Privacy and Civil Liberties Office (DPCLO), or the respective service that has the statutory authority to publish the SORN, for review and publication in the FR in accordance with 32 CFR part 310, subpart G. Following the OMB comment period, the public is given 30 days to submit written data, views, or arguments for consideration before a SOR is established or modified.

(b) *Access to Systems of Records Information.* (1) As provided by 5 U.S.C. 552a, records shall be disclosed to the individual they pertain to and under whose individual name or identifier they are filed, unless exempted by the provisions in 32 CFR part 310, subpart F, and §329.7 of this part. If an individual is accompanied by a third party, or requests a release to a third party, the individual shall be required to furnish a signed access authorization granting the third party access conditions according to 32 CFR part 310, subpart D.

(2) Individuals seeking access to records that pertain to themselves, and that are filed by their name or other personal identifier, may submit the request in person, by mail, or by email. All requests for access must be in accordance with these procedures:

(i) Any individual making a request for access to records in person shall show personal identification to the appropriate System Manager, as identified in the SORN published in the FR, to verify his or her identity, according to 32 CFR part 310, subpart D.

(ii) Any individual making a request for access to records by mail or email shall address such request to the System Manager. If the System Manager is unknown, the individual may inquire to NGB–JA/OIP: AHS-Bldg 2, Suite T319B, 111 S. George Mason Drive, Arlington, VA 22204–1382, or email *ng.ncr.arng.mbx.ngb-privacy-office@mail.mil* for assistance in locating the System Manager.

(iii) Requests for access shall include a mailing address where the records should be sent and include either a signed notarized statement or a signed unsworn declaration to verify his or her identity to ensure that they are seeking to access records about themselves and not, inadvertently or intentionally, the records of others. The Privacy Act (5 U.S.C. 552a) provides a penalty of a misdemeanor and a fine of not more than $5,000 for any person who

knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses. If making a declaration, it shall read as follows:

(A) Inside the U.S.: ''I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).''

(B) Outside the U.S.: ''I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).''

(iv) All requests for records shall describe the record sought and provide sufficient information to enable the records to be located (e.g. identification of the SORN, approximate date the record was initiated, originating organization, and type of document).

(v) All requesters shall comply with the procedures in 32 CFR part 310, subpart D for inspecting and/or obtaining copies of requested records.

(vi) Requestors affiliated with the DoD may not use official government supplies or equipment to include mailing addresses, work phones/faxes, or DoD-issued email accounts to make requests. If requests are received using DoD equipment, the requestor will be advised to make a new request, using non-DoD equipment, and processing of their request will begin only after such new request is received.

(3) The System Manager shall mail a written acknowledgement of the request for access to the individual within 10 working days of receipt. The acknowledgement shall identify the request and may, if necessary, request any additional information needed to access the record, advising the requestor that they have 20 calendar days to reply. No acknowledgement is necessary if the request can be reviewed and processed, to include notification to the individual of a grant or denial of access, within the 10 working day period. Whenever practical, the decision to grant or deny access shall be made within 30 working days. For requests presented in person, written acknowledgement may be provided at the time the request is presented.

(4) When a request for access is received, System Managers shall promptly take one of three actions on requests to access records:

(i) If no portions of the record are exempt, pursuant to the published SORN, 32 CFR part 310, subpart F, and § 329.7 of this part, the request for access shall be granted and the individual will be provided access to all records about him or her. If there is information within the record not about the record subject (e.g. third party information) that information will be removed and referred to the Chief of the OIP for processing under 5 U.S.C. 552, pursuant to 32 CFR part 286.

(ii) If the System Manager finds that the record, or portions of the record, is exempt from access pursuant to the published SORN, 32 CFR part 310, subpart F, and § 329.7 of this part, they will refer the recommended denial to the Chief of the OIP, through their Director, within 10 working days of receipt. The referral will include the following:

(A) Written recommendation for denial explaining which portion(s) of the record should be exempt from access and a discussion for why the record, or portions of the record, should be denied.

(B) The record, or portions of the record, being recommended for denial. If only portions of records are recommended for denial they must be clearly marked or highlighted.

(C) The original request and any correspondence with the requestor.

(D) A clean copy of the record.

(iii) If the request for access pertains to a record controlled and maintained by another Federal agency, but in the temporary custody of the NGB, the records are the property of the originating Component. Access to these records is controlled by the system notice and rules for the originating component/agency. Such requests shall be referred to the originating component/agency and the requestor will be notified in writing of the referral and contact information for the component/agency.

(5) The Chief of the OIP will use the following procedures for processing any recommended denials of access:

(i) The specific reason for denial cited by the System Manager will be

evaluated and a recommendation will be presented to the denial authority.

(ii) If the request for access is denied, a written letter will be sent to the requestor using procedures outlined in 32 CFR part 310, subpart D. The requestor will be advised they have 60 calendar days to appeal the decision to deny access. Appeals should be sent to: NGB Chief Counsel, 1636 Defense Pentagon, Room 1D164, Washington, DC 20301–1636. The requester must provide proof of identity or a sworn declaration with their appeal, as outlined in 32 CFR part 310, subpart D.

(iii) If the request for access should be granted, the access request will be directed back to the System Manager to process.

(6) The Chief Counsel will use the following procedures for any appeals received:

(i) The Chief Counsel will notify the Chief of the OIP that an appeal has been received and will request the administrative record of the initial denial.

(ii) The Chief of the OIP will provide an exact copy of all records from the initial denial to the Chief Counsel within 10 working days.

(iii) The Chief Counsel will review the appeal and make a final determination on whether to grant or deny the appeal.

(A) If the appellate authority denies the appeal, he or she will provide a formal written notification to the requestor using the procedures outlined in 32 CFR part 310, subpart D and will provide a copy of the response to the Chief of the OIP.

(B) If the appellate authority grants the appeal, he or she will notify the Chief of the OIP and the Directorate that recommended the denial that the individual is being given access to the record. The Chief Counsel will provide a subsequent notification to the requestor advising that his or her appeal has been granted, and will provide the requestor access to his or her record.

(iv) All appeals should be processed within 30 working days after receipt by the Chief Counsel. If the Chief Counsel determines that a fair and equitable review cannot be made within that time, the individual shall be informed in writing of the reasons for the delay and of the approximate date the review is expected to be completed.

(7) There is no requirement that an individual be given access to records that are not in a group of records that meet the definition of a SOR in 5 U.S.C. 552a.

(8) No verification of identity shall be required of an individual seeking access to records that are otherwise available to the public.

(9) Individuals shall not be denied access to a record in a SOR about themselves because those records are exempted from disclosure under 32 CFR part 285. Individuals may only be denied access to a record in a SOR about themselves when those records are exempted from the access provisions of 32 CFR part 310, subpart F, and this part.

(10) Individuals shall not be denied access to their records for refusing to disclose their Social Security Number (SSN), unless disclosure of the SSN is required by statute, by regulation adopted before January 1, 1975, or if the record's filing identifier and only means of retrieval is by the SSN (reference 5 U.S.C. 552a, note, Executive Order 9397, as amended).

(c) *Access to Records or Information Compiled for Law Enforcement Purposes.* (1) All requests by individuals to access records about themselves are processed under 5 U.S.C. 552, 5 U.S.C. 552a as well as 32 CFR part 286, 32 CFR part 310, subpart D to give requesters a greater degree of access to records on themselves, regardless of which Act is cited by the requestor for processing.

(2) Records (including those in the custody of law enforcement activities) that have been incorporated into a SOR exempted from the access conditions of 5 U.S.C. 552a and 32 CFR part 310, subpart D will be processed in accordance with 5 U.S.C. 552a, 32 CFR part 310, subpart D, and this part. Individuals shall not be denied access to records solely because they are in an exempt system. They will have the same access that they would receive under 5 U.S.C. 552 and 32 CFR part 286.

(3) Records systems exempted from access conditions will be processed under 5 U.S.C. 552 and 32 CFR part 286, or 5 U.S.C. 552a and 32 CFR part 310, subpart D, depending upon which gives the greater degree of access.

(4) If a non-law enforcement element has temporary custody of a record otherwise exempted from access under 32 CFR part 310, subpart F for the purpose of adjudication or personnel actions, they shall refer any such access request, along with the records, to the originating agency and notify the requestor of the referral.

(d) *Access to illegible, incomplete, or partially exempt records.* (1) An individual shall not be denied access to his or her record or a copy of the record solely because the physical condition or the format of the record does not make it readily available (e.g. record is in a deteriorated state or on a magnetic tape). The document will be prepared as an extract, or it will be exactly recopied.

(2) If a portion of the record contains information that is exempt from access, an extract or summary containing all of the information in the record that is releasable shall be prepared by the System Manager.

(3) When the physical condition of the record makes it necessary to prepare an extract for release, the extract shall be prepared so that the requestor will understand it.

(4) The requester shall be given access to any deletions or changes to records that are accessible.

(e) *Access to medical records.* (1) Medical records and other protected health information (PHI) shall be disclosed to the individual pursuant to Chapter 11 of DoD 6025.18–R, DoD Health Information Privacy Regulation (Available at *http://www.dtic.mil/whs/directives/corres/pdf/602518r.pdf*) and 32 CFR part 310, subpart D.

(2) The individual may be charged reproduction fees for copies or records as outlined in 32 CFR part 310, subpart D.

(f) *Amending and disputing personal information in systems of records.* (1) The System Manager shall allow individuals to request amendments to the records covered by their system notice to the extent that such records are not accurate, relevant, timely, or complete. Amendments are limited to correcting factual matters and not matters of official judgment, such as performance ratings, promotion potential, and job performance appraisals.

(2) Individuals seeking amendment to records that pertain to themselves, and that are filed or retrieved by their name or other personal identifier, may submit a request for amendment in person, by mail, or by email. All requests for amendment must be in accordance with the following:

(i) Any individual making a request for amendment to records in person shall show personal identification to the appropriate System Manager, as identified in the SORN published in the FR, to verify his or her identity, as outlined in 32 CFR part 310, subpart D.

(ii) Any individual making a request for amendment to records by mail or email shall address such request to the System Manager. If the System Manager is unknown, they may inquire to NGB–JA/OIP: AHS-Bldg 2, Suite T319B, 111 S. George Mason Drive, Arlington VA 22204–1382, or email *ng.ncr.arng.mbx.ngb-privacy-office@mail.mil* for assistance in locating the System Manager.

(iii) Requests for amendment shall include a mailing address where the decision on the request for amendment can be sent and include either a signed notarized statement or a signed unsworn declaration to verify his or her identity to ensure that they are seeking to amend records about themselves and not, inadvertently or intentionally, the records of others. The Privacy Act (5 U.S.C. 552a) provides a penalty of a misdemeanor and a fine of not more than $5,000 for any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses. The declaration shall read as follows:

(A) Inside the US: ''I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).''

(B) Outside the US: ''I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).''

(iv) All requests for amendment must include all information necessary to make a determination on the request

for amendment, as outlined in 32 CFR part 310, subpart D.

(v) Requestors affiliated with the DoD may not use official government supplies or equipment to include mailing addresses, work phones/faxes, or DoD-issued email accounts to make requests for amendment. If requests are received using DoD equipment, the requestor will be advised to make a new request, using non-DoD equipment, and processing of their request will begin only after such new request is received.

(3) When a request for amendment is received, the System Manager shall:

(i) Mail a written acknowledgement of the request for amendment to the individual within 10 working days of receipt. Such acknowledgement shall identify the request and may, if necessary, request any additional information needed to make a determination, advising the requestor that they have 20 calendar days to reply. No acknowledgement is necessary if the request can be reviewed and processed, to include notification to the individual of a grant or denial of amendment within the 10 working day period. Whenever practical, the decision to amend shall be made within 30 working days. For requests presented in person, written acknowledgement may be provided at the time the request is presented.

(ii) Determine whether the requester has adequately supported his or her claim that the record is inaccurate, irrelevant, untimely, or incomplete.

(A) If it is determined the individual's request for amendment is being granted, the System Manager will proceed to amend the records in accordance with existing statutes, regulations, or administrative procedures. The requestor will then be notified in writing of the agreement to amend and all previous holders of the records will be notified of the amendment as required by 32 CFR part 310, subpart D.

(B) If it is determined that any, or all, of the record should not be amended, the original request, along with the record requested for amendment, and justification for recommended denial action shall be forwarded through their Director to the Chief of the OIP within 10 working days of receipt for a decision by the IDA.

(C) If the request for an amendment pertains to a record controlled and maintained by another Federal agency, the amendment request shall be referred to the appropriate agency and the requestor will be notified in writing of the referral and contact information for the agency.

(4) The Chief of the OIP will use the following procedures for any recommended denials of amendment:

(i) The specific reason for denial of amendment cited by the System Manager shall be evaluated and a recommendation presented to the IDA on whether to support the recommendation to deny amendment to the record.

(ii) If the request to amend the record is denied, a written letter will be sent to the requestor using procedures outlined in 32 CFR part 310, subpart D. If an individual disagrees with the denial decision, he or she may file an appeal within 60 calendar days of receipt of the denial notification. Appeals should be sent to: NGB Chief Counsel, 1636 Defense Pentagon, Room 1D164, Washington DC 20301–1636.

(5) The Chief Counsel will use the following procedures for any appeals received:

(i) The Chief Counsel will notify Chief of the OIP that an appeal has been received and request an exact copy of the administrative record be provided within 10 working days.

(ii) The Chief Counsel will review the appeal and make a final determination on whether to grant or deny the appeal.

(A) If the Chief Counsel denies the appeal, a written letter will be provided to the requestor using the procedures outlined in 32 CFR part 310, subpart D including notification to the requestor that they may file a statement of disagreement. A brief statement will be prepared by the NGB Chief Counsel summarizing the reasons for refusing to amend the records and a copy will be provided to the Chief of the OIP and the System Manager.

(B) If the appellate authority grants the appeal, the procedures outlined in 32 CFR part 310, subpart D and this part will be followed. The System Manager will be responsible for informing all previous recipients of the amendment when a disclosure accounting has

been maintained in accordance with 32 CFR part 310, subpart E.

(iii) All appeals should be processed within 30 working days after receipt by the Chief Counsel. If the Chief Counsel determines that a fair and equitable review cannot be made within that time, the individual shall be informed in writing of the reasons for the delay and of the approximate date the review is expected to be completed.

(g) *Disclosure of disputed information.* If the appellate authority determines the record should not be amended and the individual has filed a statement of disagreement, the following procedures will be used:

(1) The System Manager that has control of the record shall annotate the disputed record so it is apparent to any person to whom the record is disclosed that a statement has been filed. Where feasible, the notation itself shall be integral to the record.

(2) Where disclosure accounting has been made, the System Manager shall advise previous recipients that the record has been disputed and shall provide a copy of the individual's statement of disagreement, and the statement summarizing the reasons for the NGB refusing to amend the records in accordance with 32 CFR part 310, subpart D.

(3) The statement of disagreement shall be maintained in a manner that permits ready retrieval whenever the disputed portion of the record is disclosed.

(4) When information that is the subject of a statement of disagreement is subsequently requested for disclosure, the System Manager will follow these procedures:

(i) The System Manager shall note which information is disputed and provide a copy of the individual's statement in the disclosure.

(ii) The System Manager shall include the summary of the NGB's reasons for not making a correction when disclosing disputed information.

(5) Copies of the statement summarizing the reasons for the NGB refusing to amend the records will be treated as part of the individual's record; however, it will not be subject to the amendment procedure outlined in 5 U.S.C. 552 and 32 CFR part 310, subpart D.

(h) *Penalties.* (1) Civil Action. An individual may file a civil suit against the NGB or its employees if the individual feels certain provisions of 5 U.S.C. 552a have been violated.

(2) Criminal Action.

(i) Criminal penalties may be imposed against any officer or employee for the offenses listed in subsection I of 5 U.S.C. 552a.

(ii) An officer or employee of NGB may be found guilty of a misdemeanor and fined up to $5,000 for a violation of the offenses listed in subsection I of 5 U.S.C. 552a.

(i) *Litigation status sheet.* Whenever a complaint citing 5 U.S.C. 552a is filed in a U.S. District Court against the NGB, or any employee of NGB, the Chief of Litigation and Employment Law shall:

(1) Promptly notify the Chief of the OIP of the complaint using the litigation status sheet in 32 CFR part 310, appendix H. This status sheet will be provided to the DPCLO, or the respective service(s) involved in the litigation.

(2) Provide a revised litigation status sheet to the Chief of the OIP at each stage of the litigation for submission to the DPCLO, or the respective service(s) involved.

(3) When a court renders a formal opinion or judgment, copies of the judgment or opinion shall be provided to the Chief of the OIP who will provide them to DPCLO, or the respective service(s) involved, along with the litigation status sheet reporting the judgment or opinion.

(j) *Computer matching programs.* All requests for participation in a matching program (either as a matching agency, or a source agency) shall be submitted directly to the DPCLO for review and compliance, following procedures in 32 CFR part 310, subpart L. The Directorate shall submit a courtesy copy of such requests to the Chief of the OIP.

§ 329.7 Exemptions.

(a) *General information.* There are two types of exemptions, general and specific. The general exemption authorizes the exemption of a SOR from all but a few requirements of 5 U.S.C. 552a. The

specific exemption authorizes exemption of a SOR or portion thereof, from only a few specific requirements. If a new SOR originates for which an exemption is proposed, or an additional or new exemption for an existing SOR is proposed, the exemption shall be submitted with the SORN. No exemption of a SOR shall be considered automatic for all records in the system. The System Manager shall review each requested records and apply the exemptions only when this will serve significant and legitimate purpose of the Federal Government.

(b) *Exemption for classified material.* All SOR maintained by the NGB 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 Executive Order 13526 and that is required by that Executive Order 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.

(c) *Exemption for anticipation of a civil action or proceeding.* All systems of records maintained by the NGB shall be exempt under section (d)(5) of 5 U.S.C. 552a, to the extent that the record is compiled in reasonable anticipation of a civil action or proceeding.

(d) *General exemptions.* No SOR within the NGB shall be considered exempt under subsection (j) or (k) of 5 U.S.C. 552a until the exemption rule for the SOR has been published as a final rule in the FR.

(e) *Specific exemptions.* (1) System identifier and name: INGB 001, Freedom of Information Act (5 U.S.C.) and Privacy Act (5 U.S.C. 552a) Case Files.

(i) Exemption: During the course of a 5 U.S.C. 552 or 5 U.S.C. 552a action, exempt materials from other systems of records may, in turn, become part of the case records in this system. To the extent that copies of exempt records from those other systems of records are entered into this 5 U.S.C. 552 or 5 U.S.C. 552a case record, the NGB hereby claims the same exemptions for the records from those other systems that are entered into this system, as claimed for the original primary SOR which they are a part.

(ii) Authority: 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), (k)(3), (k)(4), (k)(5), (k)(6), and (k)(7).

(iii) Reasons: Records are only exempt from pertinent provisions of 5 U.S.C. 552a to the extent such provisions have been identified and an exemption claimed for the original record and the purposes underlying the exemption for the original record still pertain to the record which is now contained in this SOR. In general, the exemptions were claimed in order to protect properly classified information relating to national defense and foreign policy, to avoid interference during the conduct of criminal, civil, or administrative actions or investigations, to ensure protective services provided the President and others are not compromised, to protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations, to preserve the confidentiality and integrity of Federal testing materials, and to safeguard evaluation materials used for military promotions when furnished by a confidential source. The exemption rule for the original records will identify the specific reasons why the records are exempt from specific provisions of 5 U.S.C. 552a.

(2) System identifier and name: INGB 005, Special Investigation Reports and Files.

(i) Exemption: Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information except to the extent that disclosure would reveal the identity of a confidential source. NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a SOR used in personnel or administrative actions. Any portion of this SOR which falls within

the provisions of 5 U.S.C. 552a(k)(2) may be exempt from the following subsections of 5 U.S.C. 552a: (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f).

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

(iii) Reasons: (A) From subsection (c)(3) of 5 U.S.C. 552a because to grant access to the accounting for each disclosure as required by 5 U.S.C. 552a, including the date, nature, and purpose of each disclosure and the identity of the recipient, could alert the subject to the existence of the investigation. This could seriously compromise case preparation by prematurely revealing its existence and nature; compromise or interfere with witnesses or make witnesses reluctant to cooperate; and lead to suppression, alteration, or destruction of evidence.

(B) From subsections (d) and (f) of 5 U.S.C. 552a because providing access to investigative records 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 5 U.S.C. 552a 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; enable individuals to conceal their wrongdoing or mislead the course of the investigation; 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.

(C) From subsection (e)(1) of 5 U.S.C. 552a because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(D) From subsections (e)(4)(G) and (H) of 5 U.S.C. 552a because this SOR is compiled for investigative purposes and is exempt from the access provisions of subsections (d) and (f).

(E) From subsection (e)(4)(I) of 5 U.S.C. 552a because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants.