Federal Register

Friday,
July 14, 2006

Part IV

Department of Defense

Office of the Secretary

32 CFR Part 310

Department of Defense Privacy Program; Proposed Rule

DEPARTMENT OF DEFENSE

Office of the Secretary

32 CFR Part 310

[DoD–OS–2006–129]

RIN 0790–AH98

Department of Defense Privacy Program

AGENCY: Department of Defense.

ACTION: Proposed rule.

SUMMARY: The Department of Defense is updating policies and responsibilities for the Defense Privacy Program which implements the Privacy Act of 1974.

DATES: Comments must be received on or before September 12, 2006 to be considered by this agency.

ADDRESSES: You may submit comments, identified by docket number and or RIN number and title, by any of the following methods:

- Federal eRulemaking Portal: *http://www.regulations.gov.* Follow the instructions for submitting comments.
- Mail: Federal Docket Management System Office, 1160 Defense Pentagon, Washington, DC 20301–1160.

Instructions: All submissions received must include the agency name and docket number or Regulatory Information Number (RIN) for this **Federal Register** document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at *http://regulations.gov* as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Mr. Vahan Moushegian, Jr., at (703) 607–2943.

SUPPLEMENTARY INFORMATION:

Executive Order (E.O.) 12866, ''Regulatory Planning and Review''

It has been determined that 32 CFR part 310 is not a significant regulatory action. The rule does not (1) Have an annual effect on the economy of $100 million or more or adversely affect in a material way the economy; a sector of the economy; productivity; competition; jobs; the environment; public health or safety; or State, local, or tribal governments or communities; (2) Create a serious inconsistency or otherwise interfere with an action taken or planned by another Agency; (3) Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs, or the rights and obligations of recipients thereof; or (4) Raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in this Executive order.

Public Law 96–354, ''Regulatory Flexibility Act'' (5 U.S.C. Chapter 6)

It has been determined that this rule is not subject to the Regulatory Flexibility Act because it would not, if promulgated, have a significant economic impact on a substantial number of small entities because it is only concerned with the administration of Privacy Program within the Department of Defense.

Public Law 96–511, ''Paperwork Reduction Act'' (44 U.S.C. Chapter 35)

It has been determined that this rule does not impose information requirements beyond the Department of Defense and that the information collected within the Department of Defense is necessary and consistent with 5 U.S.C. 552a, known as the Privacy Act of 1974. However, one favorable comment was forwarded to the Office of Management and Budget during the 30-day review period (71 FR 29319).

Section 202, Public Law 104–4, ''Unfunded Mandates Reform Act''

It has been determined that the rule does not involve a Federal mandate that may result in the expenditure by State, local and tribal governments, in the aggregate, or by the private sector, of $100 million or more in any one year.

Executive Order 13132, ''Federalism''

It has been determined that this rule does not have federalism implications. The rule does not have substantial direct effects on the States, the relationship between the National Government and the States, or on the distribution of power and responsibilities among the various levels of government.

List of Subjects in 32 CFR Part 310

DoD privacy program.

Accordingly, 32 CFR part 310 is proposed to be revised as follows.

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

Subpart A—DoD Policy

§ 310.1 Reissuance.

This part is revised to consolidate into a single document (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 policies and responsibilities of the DoD Privacy Program under 5 U.S.C. 552a and OMB Circular A–130.

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

(c) Continues to authorize the publication of DoD 5400.11–R.

(d) Continues to delegate authorities and responsibilities for the effective administration of the DoD Privacy Program.

§ 310.3 Applicability and Scope.

This part:

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

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

(c) This part does not apply to:

(1) Requests for information made under the Freedom of Information Act. They are processed in accordance with DoD 5400.7–R.[3]

(2) Requests for information from systems of records controlled by the Office of Personnel Management (OPM), although maintained by a DoD Component. These are processed in accordance with policies established by OPM ''Privacy Procedures for Personnel Records'' (5 CFR 297).

(3) Requests for personal information from the General Accounting Office. These are processed in accordance with DoD Directive 7650.1.[4]

(4) Requests for personal information from Congress. These are processed in accordance with DoD Directive 5400.4 except those specific provisions in Subpart E-Disclosure of Personal Information to Other Agencies and Third Parties.

§ 310.4. 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) *Agency.* For the purposes of disclosing records subject to the Privacy Act among the DoD Components, the Department of Defense is a 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.

(c) *Computer Matching Program.* The computerized comparison of two or more automated systems of records or a system of records with non-Federal records. Manual comparison of systems of records or a system of records with non-Federal records are not covered.

(d) *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.

(e) *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.

(f) *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.

(g) *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).

(h) *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.).

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

(j) *Lost, stolen, or compromised information.* Actual or possible disclosure of personal information either to known or unknown persons whether or not a potential exists that the information may be used for unlawful purposes to the detriment of the individual.

(k) *Maintain.* To maintain, collect, use, or disseminate records contained in a system of records.

(l) *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.

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

[2] See footnote 1 to § 310.1.

[3] See footnote 1 to § 310.3 (c)(1).

[4] See footnote 1 to § 310.3 (c)(1).

(m) *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.[5]

(n) *Personal information.* Information about an individual that identifies, relates, or 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, personnel, medical, and financial information; etc.

(o) *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.

(p) *Member of the public.* Any individual or party acting in a private capacity to include Federal employees or military personnel.

(q) *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.

(r) *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.

(s) *Risk assessment.* An analysis considering information sensitivity, vulnerabilities, and cost in safeguarding personal information processed or stored in the facility or activity.

(t) *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.

(u) *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.

(v) *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.

(w) *System of records.* A group of records under the control of a DoD 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.

§ 310.5 Policy.

It is DoD policy that:

(a) The privacy of an individual is a personal and fundamental right that shall be respected and protected.

(1) The Department's need to collect, maintain, use, or disseminate personal information about individuals for purposes of discharging its statutory responsibilities shall be balanced against the right of the individual to be protected against unwarranted invasions of their privacy.

(2) The legal rights of individuals, as guaranteed by Federal law, regulation, and policy, shall be protected when collecting, maintaining, using, or disseminating personal information about individuals.

(3) DoD personnel, including contractors, have an affirmative responsibility to protect an individual's privacy when collecting, maintaining, using, or disseminating personal information about an individual.

(4) Departmental legislative, regulatory, or other policy proposals shall be evaluated to ensure that privacy implications, including those relating to the collection, maintenance, use, or dissemination of personal information, are assessed, to include, when required and consistent with the Privacy Provision of the E-Government Act of 2002 (44 U.S.C. 3501, Note), the preparation of a Privacy Impact Assessment.

(b) Personal information shall be collected, maintained, used, or disclosed to ensure that:

(1) It shall be relevant and necessary to accomplish a lawful DoD purpose required to be accomplished by statute or Executive order.

(2) It shall be collected to the greatest extent practicable directly from the individual.

(3) 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 that information.

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

(5) 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.

(c) No record shall be maintained on how an individual exercises rights guaranteed by the First Amendment to the Constitution, except as follows:

(1) Specifically authorized by statute.

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

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

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

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

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

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

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

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

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

(g) Disclosure of records pertaining to personnel of the National Security Agency, the Defense Intelligence Agency, the National Reconnaissance

[5] 5 See footnote 1 to § 310.1.

Office, and the National Geospatial-Intelligence Agency shall be prohibited to the extent authorized by Public Law 86–36 (1959) and 10 U.S.C. 424. Disclosure of records pertaining to personnel of overseas, sensitive, or routinely deployable units shall be prohibited to the extent authorized by 10 U.S.C. 130b. Disclosure of medical records is prohibited except as authorized by DoD 6025.18–R. [6]

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

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

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

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

§ 310.6 Responsibilities.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(5) Assess the impact of technology on the privacy of personal information and, when feasible, adopt privacy enhancing technology both to preserve and protect personal information contained in Component systems of records and to permit auditing of compliance with the requirements of this part and DoD 5400.11–R.

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

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

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

§ 310.7 Information requirements.

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

§ 310.8 Rules of conduct.

(a) DoD personnel shall:

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

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

(3) Report any unauthorized disclosures of personal information from a system of records or the maintenance of any system of records that are not authorized by this part to the applicable Privacy POC for his or her DoD Component.

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

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

(2) Prepare promptly any required new, amended, or altered system notices for the system of records and submit them through their DoD Component Privacy POC to the DPO for publication in the **Federal Register**.

(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 DoD 5400.11–R, is subject to possible criminal penalties and/or administrative sanctions.

[6] See footnote 1 to § 310.1.

[7] See footnote 1 to § 310.1.

§ 310.9 Privacy boards and office, composition and responsibilities.

(a) *The Defense Privacy Board*—(1) *Membership.* The Board shall consist of the DA&M, OSD, who shall serve as the Chair; the Director of the DPO, DA&M, who shall serve as the Executive Secretary and as a member; the representatives designated by the Secretaries of the Military Departments; and the following officials or their designees: the Deputy Under Secretary of Defense for Program Integration (DUSD(PI)); the Assistant Secretary of Defense for Health Affairs; the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)/Chief Information Officer (CIO); the Director, Executive Services and Communications Directorate, WHS; the GC, DoD; and the Director for Information Technology Management Directorate (ITMD), WHS. The designees also may be the principal POC for the DoD Component for privacy matters.

(2) *Responsibilities.* (i) The Board shall have oversight responsibility for implementation of the DoD Privacy Program. It shall ensure the policies, practices, and procedures of that Program are premised on the requirements of 5 U.S.C. 552a and OMB Circular A–130, as well as other pertinent authority, and the Privacy Programs of the DoD Component are consistent with, and in furtherance of, the DoD Privacy Program.

(ii) The Board shall serve as the primary DoD policy forum for matters involving the DoD Privacy Program, meeting as necessary, to address issues of common concern so as to ensure uniform and consistent policy shall be adopted and followed by the DoD Components. The Board shall issue advisory opinions as necessary on the DoD Privacy Program so as to promote uniform and consistent application of 5 U.S.C. 552a, OMB Circular A–130, and DoD 5400.11–R.

(iii) Perform such other duties as determined by the Chair or the Board.

(b) *The Defense Data Integrity Board*—(1) *Membership.* The Board shall consist of the DA&M, OSD, who shall serve as the Chair; the Director of the DPO, DA&M, who shall serve as the Executive Secretary; and the following officials or their designees: the representatives designated by the Secretaries of the Military Departments; the DUSD(PI); the ASD(NII)/CIO; the GC, DoD; the Inspector General, DoD; the ITMD, WHS; and the Director, Defense Manpower Data Center. The designees also may be the principal points of contact for the DoD Component for privacy matters.

(2) *Responsibilities.* (i) The Board shall oversee and coordinate, consistent with the requirements of 5 U.S.C. 552a, OMB Circular A–130, and DoD 5400.11–R, all computer matching programs involving personal records contained in system of records maintained by the DoD Components.

(ii) The Board shall review and approve all computer matching agreements between the Department of Defense and the other Federal, State or local governmental agencies, as well as memoranda of understanding when the match is internal to the Department of Defense, to ensure, under 5 U.S.C. 552a, OMB Circular A–130, and DoD 5400.11–R, appropriate procedural and due process requirements shall have been 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) 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) 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 submission of required match notices for publication in the **Federal Register** and advance notification to the OMB and the Congress of the proposed matches, 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 references OMB Circular A–130 and DoD 5400.11–R, and such other reports as may be required.

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

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'' 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 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 are rearranged in such 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 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 for performing 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.* Establish appropriate administrative, technical and physical safeguards to ensure the records in each system of records are protected from unauthorized access, alteration, or disclosure and 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 in accordance with reference 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 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.

(2) The transfer of large quantities of records containing personal data in bulk to a disposal activity, such as the Defense Property Disposal Office, is not a release of personal information under this part. The sheer volume of such transfers make it difficult or impossible to identify readily specific individual records (see paragraph (c)(3) of this section).

(3) When disposing of or destroying large quantities of records containing personal information, care must be exercised to ensure the bulk of the records are maintained so as to prevent specific records from being readily identified. If bulk is maintained, no special procedures are required. If bulk cannot be maintained or if the form of the records makes individually identifiable information easily available, dispose of the record in accordance with paragraph (c)(1) of this section.

§ 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 will be severe if the records are misused. To assist the individual, the Component shall notify the individual of any loss, theft, or compromise.

(1) The notification shall be made whenever information pertaining to a service member, civilian employee (appropriated or non-appropriated fund), military retiree, family member, DoD contractor, or any other person that is affiliated with the Component (*e.g.*, volunteer) is involved (See § 310.50).

(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) Notification to the Deputy Secretary shall be forwarded to the Component Privacy Official, who shall forward it to the DPO. The DPO, 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.

(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.

(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 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 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.

[8] See footnote 1 to § 310.1.

(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 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 that 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, unless 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. This determination shall be made in consultation with a medical doctor.

(3) If it is determined that the release of the medical information may be harmful to the mental or physical health of the individual or to a third party:

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

(ii) 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).

(4) Do not require the physician to request the records for the individual.

(5) 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).

(6) 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.

(7) Access to a minor's medical records may be granted to his or her parents or legal guardians. However, access may be subject to one or more of the below restrictions:

(i) In the United States, the laws of the particular State in which the records are located may afford special protection to certain types of medical records (for example, records dealing with treatment for drug or alcohol abuse and certain psychiatric records). Even if the records are maintained by a military medical facilities these statutes may apply.

(ii) For the purposes of parental access to the medical records and medical determinations regarding minors at overseas installation the age of majority is 18 years except when:

(A) A minor at the time he or she sought or consented to the treatment was between 15 and 17 years of age;

(B) The treatment was sought in a program that was authorized by regulation or statute to offer confidentiality of treatment records as a part of the program;

(C) The minor specifically requested or indicated that he or she wished the treatment record to be handled with confidence and not released to a parent or guardian; and

(D) The parent or guardian seeking access does not have the written authorization of the minor or a valid court order granting access.

(iii) If all four of the above conditions are met, the parent or guardian shall be denied access to the medical records of the minor. Do not use these procedures to deny the minor access to his or her own records under this part or any other statutes.

(8) All members of the Military Services and all married persons are not considered minors regardless of age, and the parents of these individuals 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 record has been exempted specifically from the amendment procedures of this Regulation 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 that:

(1) The appeal, with all supporting material, both that furnished by 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 that:

(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 part 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 waiver 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 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 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*) Position descriptions.

(B) All disclosures of personal information regarding Federal civilian employees shall be made in accordance with OPM release policies (see 5 CFR 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 routine uses established for each of the individual system notices, blanket routine uses have been established (see Appendix C) are applicable to all DoD system of records. These blanket routine uses are published only at the beginning of the listing of system notices for each Component in the **Federal Register**. Each system notice shall expressly state whether or not the blanket routine uses apply to the system of records.

(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 Record 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 and the GAO.* (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. Records may also be disclosed to the GAO in the course of the activities of GAO.

(2) The blanket routine use for ''Congressional Inquiries'' (see Appendix C, Section D) applies to all systems; therefore, there is no need to verify that the individual has authorized the release of his or her record to a congressional member when responding to a congressional constituent inquiry.

(3) 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.

(4) The verbal statement by a Congressional staff member is acceptable to establish that a request has been received from the person to whom the records pertain.

(5) If the constituent inquiry is being made on behalf of someone other than the individual to whom the record pertains, provide the Congressional member only information releasable under 32 CFR part 286. Advise the Congressional member that the written consent of the individual to whom the record pertains is required before any additional information may be released. Do not contact individuals to obtain their consents for release to Congressional members unless a Congressional office specifically requests that this be done.

(6) Nothing in paragraph (i)(2) 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.

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

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

(j) *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.

(k) *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 (k)(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 are 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 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 general nor specific exemptions are 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 provisions 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.* (1) 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).

(2) DoD Components shall consult with the DPO before initiating action to claim either a general or specific exemption for any system of records.

(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) The term ''civil action or proceeding'' is intended to include

court proceedings or quasi-judicial administrative hearings or proceedings.

(b) Any information prepared in conjunction with judicial or quasi-judicial, either before or incident to the, proceedings, to include information prepared to advise the DoD Component officials of the possible legal or other consequences of a given course of action, are protected.

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

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

§ 310.28 General exemption.

(a) 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 include 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) 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 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 by reference 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 Office of General Counsel, DoD. 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) Section 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.

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

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

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

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

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

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

[9] See footnote 1 to § 310.1.

[10] See footnote 1 to § 310.1.

(xv) 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 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 information contained in the system was obtained, e.g., the individual, other Component documentation, other Federal agencies, etc).

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

(p) *System Exempted From Certain Provisions of the Act.* (1) If no exemption has been claimed for the system, indicate ''None.''

(2) If there is an exemption claimed indicate specifically under which section of the Privacy Act it is claimed.

(3) Cite the CFR section containing the exemption rule for the system. For example, ''An exemption rule for this system has been promulgated and published in 32 CFR 311'').

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

(2) Coordinate with the DPO to ensure that all new systems are added to the master registry and all amendments and alterations are incorporated into the master registry.

(3) 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, and inform their personnel of 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 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.

§ 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 the Privacy Act (5 U.S.C. 552a) are sensitive to the requirements of this part, especially the access, use, and dissemination restrictions. Though not required, Components shall give consideration to whether annual certification should be mandated for certain personnel whose duties and responsibilities require daily interaction with privacy protected information.

(d) Components shall conduct training that reaches the widest possible audience. The use of Web-based training or video conferencing training are means by which such training can be conducted that has proven effective.

§ 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 cost, 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 Component shall immediately notify the DPO.

(b) The Component shall conduct an inquiry into the facts and circumstances surrounding the compromise and shall provide the DPO a copy of the final report.

(c) The Component shall determine what remedial actions must be taken to prevent a similar loss in the future. The Component shall also 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 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 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 record, 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—Special Considerations for Safeguarding Personal Information Technology (IT) Systems

(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.[11]

2. Personal 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 part. However, all unclassified information subject to this part 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, ''Management of Federal Information Resources.''

2. Technical and physical safeguards alone will not protect against unintentional compromise due to errors, omissions, or poor procedures. Proper administrative controls generally provide cheaper and surer safeguards.

3. 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 DoD 5200.1–R satisfies this requirement.

3. Mark and protect all computer products containing classified data in accordance with DoD 5200.1–R and DoD Directive 8500.1.

[11] See footnote 1 to § 310.1.

4. Mark and protect all computer products containing ''For Official Use Only'' material in accordance with DoD 5200.1–R.

5. Ensure 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 all IT personnel involved in processing information subject to this part 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 part 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.

E. Technical Safeguards

1. The use of encryption devices solely for the purpose of protecting unclassified personal information transmitted over secure communication circuits or during processing in computer systems is normally discouraged. However, when a comprehensive risk assessment indicates encryption is cost-effective, it may be used.

2. Remove personal data stored on magnetic storage media by methods that preclude reconstruction of the data.

3. Ensure personal information is not inadvertently disclosed as residue when transferring magnetic media between activities.

4. When it is necessary to provide dial-up remote access for the processing of personal information, control access by computer-verified passwords. Change passwords periodically or whenever compromise is known or suspected.

5. Normally the passwords shall give access only to those data elements (fields) required and not grant access to the entire database.

6. Do not totally rely on proprietary software products to protect personnel data during processing or storage.

F. Special Procedures

1. System Managers shall:

a. Notify the IT manager whenever personal information subject to this part is to be processed by an IT facility.

b. Prepare and submit for publication all system notices and amendments and alterations thereto. (see § 310.30(f)).

c. Identify to the IT manager those activities and individuals authorized access to the information and notify the manager of any changes to the access authorizations.

d. If required, IT managers shall ensure a Privacy Impact Assessment is prepared consistent with the requirements of 44 U.S.C. 3501 Note (section 208, ''Privacy Provisions,'' E-Government Act of 2002).

2. IT Personnel shall:

a. Permit only authorized individuals access to the information.

b. Adhere to the established information protection procedures and rules of conduct.

c. Notify the system manager and IT manager whenever unauthorized personnel seek access to the information.

3. IT Installation Managers shall:

a. Maintain an inventory of all computer program applications used to process information subject to this part to include the identity of the systems of records involved.

b. Verify that requests for new programs or changes to existing programs have been published as required. (see paragraphs (a) and (b) of § 310.33).

c. Notify the system manager whenever changes to computer installations, communications networks, or any other changes in the IT environment occur that require an altered system report be submitted. (see § 310.33(b)).

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.

2. Do not use respliced waste computer products containing personal data.

H. Risk Assessment for IT Installations That Process Personal Data

1. A separate risk assessment is not required for IT activities that process classified material. A simple certification by the appropriate IT official that the facility is cleared to process a given level of classified material (such as Top Secret, Secret, or Confidential) and that the procedures followed in processing ''For Official Use Only'' material are to be followed in processing personal data subject to this part is sufficient to meet the risk assessment requirement.

2. Prepare a formal risk assessment, as necessary, for each IT activity (to include those activities with terminals and IT devices) that processes personal information subject to this part and that do not process classified material.

3. Address the following in the risk assessment:

a. Identify the specific systems of records supported and determine their impact on the mission of the user.

b. Identify the threats (internal, external, and natural) to the data.

c. Determine the physical and operational (to include software) vulnerabilities.

d. Evaluate the relationships between vulnerabilities and threats.

e. Assess the impact of unauthorized disclosure or modification of the personal information.

f. Identify possible safeguards and their relationships to the threats to be countered.

g. Analyze the economic feasibility of adopting the identified safeguards.

h. Determine the safeguard to be used and develop implementation plans.

i. Discuss contingency plans including operational exercise plans.

j. Determine if procedures proposed are consistent with those identified in the system notices for system of records concerned.

k. Include a vulnerability assessment.

4. The risk assessment shall be reviewed by the appropriate Component officials.

5. Conduct a risk assessment at least as frequently as considered necessary or when there is a change to the installation, its hardware, software, or administrative procedures that increase or decrease the likelihood of compromise or present new threats to the information.

6. Protect the risk assessment, as it is a sensitive document.

7. Retain a copy of the risk assessment at the installation and make it available to appropriate inspectors and authorized personnel.

8. Include a summary of the current risk assessment with any report of new or altered system submitted in accordance with § 310.33(c) for any system from which information will be processed.

9. Complete a formal risk assessment at the beginning of the design phase for each new unclassified IT installation and before beginning the processing of personal data on a regular basis in existing IT facilities that do not process classified 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, D.C. 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 e-mail 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. And because the information in the laptop was password protected, 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.

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. 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.
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 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: Records maintained 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, 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.

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 for 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 define 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 e-mail 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 Attach 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)

[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).

7. Court Action
a. Court's Finding
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)

Dated: June 29, 2006.

L.M. Bynum,

OSD Federal Register Liaison Officer, DOD.

[FR Doc. 06–6011 Filed 7–13–06; 8:45 am]

BILLING CODE 5001–06–P