

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 Number¹
2. Requester
3. Document Title or Description²
4. Litigation
 - a. Date Complaint Filed
 - b. Court
 - c. Case File Number¹
5. Defendants (DoD Component and individual)
6. Remarks (brief explanation of what the case is about)
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)

PART 311—OFFICE OF THE SECRETARY OF DEFENSE AND JOINT STAFF PRIVACY PROGRAM

Sec.

- 311.1 Purpose.
- 311.2 Applicability.
- 311.3 Definitions.
- 311.4 Policy.
- 311.5 Responsibilities.
- 311.6 Procedures.
- 311.7 OSD/JS Privacy Office Processes.
- 311.8 Procedures for exemptions.

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

SOURCE: 74 FR 56114, Oct. 30, 2009, unless otherwise noted.

¹Number used by the Component for reference purposes.

²Indicate the nature of the case, such as, "Denial of access," "Refusal to amend," "Incorrect records," or other violations of the Act (specify).

§ 311.1

32 CFR Ch. I (7–1–11 Edition)

§ 311.1 Purpose.

This part revises 32 CFR part 311 to update Office of the Secretary of Defense (OSD) and Joint Staff (JS) policy, assigns responsibilities, and prescribes procedures for the effective administration of the Privacy Program in OSD and the JS. This part supplements and implements part 32 CFR part 310, the DoD Privacy Program.

§ 311.2 Applicability.

This part:

(a) Applies to OSD, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, and all other activities serviced by Washington Headquarters Services (WHS) that receive privacy program support from OSD/JS Privacy Office, Executive Services Directorate (ESD), WHS (hereafter referred to collectively as the “WHS-Serviced Components”).

(b) Covers systems of records maintained by the WHS-Serviced Components and governs the maintenance, access, change, and release information contained in those systems of records, from which information about an individual is retrieved by a personal identifier.

§ 311.3 Definitions.

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

(b) *Computer matching program*. A program that matches the personal records in computerized databases of two or more Federal agencies.

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

(d) *Individual*. A living person who is a citizen of the United States or an alien lawfully admitted for permanent residence. The parent of a minor or the legal guardian of any individual also may act on behalf of an individual. Members of the United States Armed Forces are “individuals.” Corporations, partnerships, sole proprietorships, professional groups, businesses, whether

incorporated or unincorporated, and other commercial entities are not “individuals” when acting in an entrepreneurial capacity with the Department of Defense but are “individuals” otherwise (*e.g.*, security clearances, entitlement to DoD privileges or benefits, *etc.*).

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

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

(g) *Personal information*. Information about an individual that identifies, links, relates, or is unique to, or describes him or her, *e.g.*, a social security number; age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information, *etc.* Such information also is known as *personally identifiable information* (*i.e.*, information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, date and place of birth, mother’s maiden name, biometric records, including any other personal information which is linked or linkable to a specified individual).

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

(i) *System manager*. A WHS-Serviced Component official who has overall responsibility for a system of records. The system manager may serve at any level in OSD. Systems managers are indicated in the published systems of records notices. If more than one official is indicated as a system manager, initial responsibility resides with the manager at the appropriate level (*i.e.*, for local records, at the local activity).

(j) *System of records.* A group of records under the control of a WHS-Serviced Component from which personal information about an individual is retrieved by the name of the individual or by some other identifying number, symbol, or other identifying particular assigned, that is unique to the individual.

§311.4 Policy.

It is DoD policy, in accordance with 32 CFR part 310, that:

(a) Personal information contained in any system of records maintained by any DoD organization shall be safeguarded. To the extent authorized by section 552a of title 5, United States Code, commonly known and hereafter referred to as the "Privacy Act" and Appendix I of Office of Management and Budget Circular No. A-130 (available at <http://www.whitehouse.gov/omb/assets/omb/circulars/a130/a130trans4.pdf>), an individual shall be permitted to know what existing records pertain to him or her consistent with 32 CFR part 310.

(b) Each office maintaining records and information about individuals shall ensure that this data is protected from unauthorized collection, use, dissemination and/or disclosure of personal information. These offices shall permit individuals to have access to and have a copy made of all or any portion of records about them, except as provided in 32 CFR 310.17 and 310.18. The individuals will also have an opportunity to request that such records be amended as provided by 32 CFR 310.19. Individuals requesting access to their records shall receive concurrent consideration under section 552 of title 5, United States Code (commonly known and hereafter referred to as the "Freedom of Information Act").

(c) Necessary records of a personal nature that are individually identifiable will be maintained in a manner that complies with the law and DoD policy. Any information collected by WHS-Serviced Components must be as accurate, relevant, timely, and complete as is reasonable to ensure fairness to the individual. Adequate safeguards must be provided to prevent misuse or unauthorized release of such information, consistent with the Privacy Act.

§311.5 Responsibilities.

(a) The Director, WHS, under the authority, direction, and control of the Director, Administration and Management, shall:

(1) Direct and administer the OSD/JS Privacy Program for the WHS-Serviced Components.

(2) Ensure implementation of and compliance with standard and procedures established in 32 CFR part 310.

(3) Coordinate with the WHS General Counsel on all WHS-Serviced Components denials of appeals for amending records and review actions to confirm denial of access to records.

(4) Provide advice and assistance to the WHS-Serviced Components on matters pertaining to the Privacy Act.

(5) Direct the OSD/JS Privacy Office to implement all aspects of 32 CFR part 310 as directed in §311.7 of this part.

(b) The Heads of the WHS-Serviced Components shall:

(1) Designate an individual in writing as the point of contact for Privacy Act matters and advise the Chief, OSD/JS Privacy Office, of names of officials so designated.

(2) Designate an official in writing to deny initial requests for access to an individual's records or changes to records and advise the Chief, OSD/JS Privacy Office of names of officials so designated.

(3) Provide opportunities for appointed personnel to attend periodic Privacy Act training.

(4) Report any new record system, or changes to an existing system, to the Chief, OSD/JS Privacy Office at least 90 days before the intended use of the system.

(5) Formally review each system of records notice on a biennial basis and update as necessary.

(6) In accordance with 32 CFR 310.12, include appropriate Federal Acquisition Regulation clause (48 CFR 24.104) in all contracts that provide for contractor personnel to access WHS-Serviced Component records systems covered by the Privacy Act.

(7) Review all implementing guidance prepared by the WHS-Serviced Components as well as all forms or other methods used to collect information about individuals to ensure compliance with 32 CFR part 310.

§311.6

32 CFR Ch. I (7–1–11 Edition)

(8) Establish administrative processes in WHS-Serviced Component organizations to comply with the procedures listed in this part and 32 CFR part 310.

(9) Coordinate with WHS General Counsel on all proposed denials of access to records.

(10) Provide justification to the OSD/JS Privacy Office when access to a record is denied in whole or in part.

(11) Provide the record to the OSD/JS Privacy Office when the initial denial of a request for access to such record has been appealed by the requester or at the time of initial denial if an appeal seems likely.

(12) Maintain an accurate administrative record documenting the actions resulting in a denial for access to a record or for the correction of a record. The administrative record should be maintained so it can be relied upon and submitted as a complete record of proceedings if litigation occurs in accordance with 32 CFR part 310.

(13) Ensure all personnel are aware of the requirement to take appropriate Privacy Act training as required by 32 CFR part 310 and the Privacy Act.

(14) Forward all requests for access to records received directly from an individual to the OSD/JS Freedom of Information Act Requester Service Center for processing under 32 CFR part 310 and 32 CFR part 286.

(15) Maintain a record of each disclosure of information (other than routine use) from a system of records as required by 32 CFR part 310.

§311.6 Procedures.

(a) *Publication of Notice in the FEDERAL REGISTER.* (1) A notice shall be published in the FEDERAL REGISTER of any record system meeting the definition of a system of records in 32 CFR 310.4.

(2) The Heads of the WHS-Serviced Component shall submit notices for new or revised systems of records to the Chief, OSD/JS Privacy Office, for review at least 90 days prior to desired implementation.

(3) The Chief, OSD/JS Privacy Office shall forward completed notices to the Defense Privacy Office (DPO) for review in accordance with 32 CFR 310.30. Publication in the FEDERAL REGISTER

starts a 30-day comment window which provides the public with an opportunity to submit written data, views, or arguments to the DPO for consideration before a system of record is established or modified.

(b) *Access to Systems of Records Information.* (1) As provided in the Privacy Act, records shall be disclosed only to the individual they pertain to and under whose individual name or identifier they are filed, unless exempted by the provisions in 32 CFR 310.31. If an individual is accompanied by a third party, the individual shall be required to furnish a signed access authorization granting the third party access according to 32 CFR 310.17.

(2) Individuals seeking access to records that pertain to themselves, and that are filed by name or other personal identifier, may submit the request in person or by mail, in accordance with these procedures:

(i) Any individual making a request for access to records in person shall provide personal identification to the appropriate system owner, as identified in the system of records notice published in the FEDERAL REGISTER, to verify the individual's identity according to 32 CFR 310.17.

(ii) Any individual making a request for access to records by mail shall address such request to the OSD/JS FOIA Requester Service Center, Office of Freedom of Information, 1155 Pentagon, Washington, DC 20301-1155. To verify his or her identity, the requester shall include either a signed notarized statement or an unsworn declaration in the format specified by 32 CFR part 286.

(iii) All requests for records shall describe the record sought and provide sufficient information to enable the material to be located (*e.g.*, identification of system of records, approximate date it was initiated, originating organization, and type of document).

(iv) All requesters shall comply with the procedures in 32 CFR part 310 for inspecting and/or obtaining copies of requested records.

(v) If the requester is not satisfied with the response, he or she may file a written appeal as provided in paragraph (f)(8) of this section. The requester must provide proof of identity

by showing a driver's license or similar credentials.

(3) There is no requirement that an individual be given access to records that are not in a group of records that meet the definition of a system of records in the Privacy Act. (For an explanation of the relationship between the Privacy Act and the Freedom of Information Act, and for guidelines to ensure requesters are given the maximum amount of information authorized by both Acts, see 32 CFR part 310.17)

(4) Granting access to a record containing personal information shall not be conditioned upon any requirement that the individual state a reason or otherwise justify the need to gain access.

(5) No verification of identity shall be required of an individual seeking access to records that are otherwise available to the public.

(6) Individuals shall not be denied access to a record in a system of records about themselves because those records are exempted from disclosure under 32 CFR part 286. Individuals may only be denied access to a record in a system of records about themselves when those records are exempted from the access provisions of 32 CFR 310.26.

(7) Individuals shall not be denied access to their records for refusing to disclose their Social Security Number (SSN), unless disclosure of the SSN is required by statute, by regulation adopted before January 1, 1975, or if the record's filing identifier and only means of retrieval is by SSN (Privacy Act, note).

(c) *Access to Records or Information Compiled for Law Enforcement Purposes.*

(1) Requests are processed under 32 CFR part 310 and 32 CFR part 286 to give requesters a greater degree of access to records on themselves.

(2) Records (including those in the custody of law enforcement activities) that have been incorporated into a system of records exempted from the access conditions of 32 CFR part 310, will be processed in accordance with 32 CFR 286.12. Individuals shall not be denied access to records solely because they are in the exempt system. They will have the same access that they would receive under 32 CFR part 286. (See also 32 CFR 310.17.)

(3) Records systems exempted from access conditions will be processed under 32 CFR 310.26 or 32 CFR 286.12, depending upon which regulation gives the greater degree of access. (See also 32 CFR 310.17.)

(4) Records systems exempted from access under 32 CFR 310.27 that are temporarily in the hands of a non-law enforcement element for adjudicative or personnel actions, shall be referred to the originating agency. The requester will be informed in writing of this referral.

(d) *Access to Illegible, Incomplete, or Partially Exempt Records.* (1) An individual shall not be denied access to a record or a copy of a record solely because the physical condition or format of the record does not make it readily available (e.g., deteriorated state or on magnetic tape). The document will be prepared as an extract, or it will be exactly recopied.

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

(3) When the physical condition of the record makes it necessary to prepare an extract for release, the extract shall be prepared so that the requester will understand it.

(4) The requester shall be informed of all deletions or changes to records.

(e) *Access to Medical Records.* (1) Medical records shall be disclosed to the individual and may be transmitted to a medical doctor named by the individual concerned.

(2) The individual may be charged reproduction fees for copies or records as outlined in 32 CFR 310.20.

(f) *Amending and Disputing Personal Information in Systems of Records.*

(1) The Head of a WHS-Serviced Component, or designated official, shall allow individuals to request amendment to their records to the extent that such records are not accurate, relevant, timely, or complete.

(2) Requests shall be submitted in person or by mail to the office designated in the system of records notice. They should contain, as a minimum, identifying information to locate the record, a description of the items to be

§ 311.6

32 CFR Ch. I (7-1-11 Edition)

amended, and the reason for the change. Requesters shall be required to provide verification of their identity as stated in paragraphs (b)(2)(i) and (b)(2)(ii) of this section to ensure that they are seeking to amend records about themselves and not, inadvertently or intentionally, the records of others.

(3) Requests shall not be rejected nor required to be resubmitted unless additional information is essential to process the request.

(4) The appropriate system manager shall mail a written acknowledgment to an individual's request to amend a record within 10 workdays after receipt. Such acknowledgment shall identify the request and may, if necessary, request any additional information needed to make a determination. No acknowledgment is necessary if the request can be reviewed and processed and if the individual can be notified of compliance or denial within the 10-day period. Whenever practical, the decision shall be made within 30 working days. For requests presented in person, written acknowledgment may be provided at the time the request is presented.

(5) The Head of a WHS-Serviced Component, or designated official, shall promptly take one of three actions on requests to amend the records:

(i) If the WHS-Serviced Component official agrees with any portion or all of an individual's request, he or she will proceed to amend the records in accordance with existing statutes, regulations, or administrative procedures and inform the requester of the action taken in accordance with 32 CFR 310.19. The WHS-Serviced Component official shall also notify all previous holders of the record that the amendment has been made and shall explain the substance of the correction.

(ii) If the WHS-Serviced Component official disagrees with all or any portion of a request, the individual shall be informed promptly of the refusal to amend a record, the reason for the refusal, and the procedure to submit an appeal as described in paragraph (f)(8) of this section.

(iii) If the request for an amendment pertains to a record controlled and maintained by another Federal agency,

the request shall be referred to the appropriate agency and the requester advised of this.

(6) When personal information has been disputed by the requestor, the Head of a WHS-Serviced Component, or designated official, shall:

(i) Determine whether the requester has adequately supported his or her claim that the record is inaccurate, irrelevant, untimely, or incomplete.

(ii) Limit the review of a record to those items of information that clearly bear on any determination to amend the record, and shall ensure that all those elements are present before a determination is made.

(7) If the Head of a WHS-Serviced Component, or designated official, after an initial review of a request to amend a record, disagrees with all or any portion of the request to amend a record, he or she shall:

(i) Advise the individual of the denial and the reason for it.

(ii) Inform the individual that he or she may appeal the denial.

(iii) Describe the procedures for appealing the denial, including the name and address of the official to whom the appeal should be directed. The procedures should be as brief and simple as possible.

(iv) Furnish a copy of the justification of any denial to amend a record to the OSD/JS Privacy Office.

(8) If an individual disagrees with the initial WHS-Serviced Component determination, he or she may file an appeal. If the record is created and maintained by a WHS-Serviced Component, the appeal should be sent to the Chief, OSD/JS Privacy Office, WHS, 1155 Defense Pentagon, Washington, DC 20301-1155.

(9) If, after review, the Chief, OSD/JS Privacy Office, determines the system of records should not be amended as requested, the Chief, OSD/JS Privacy Office, shall provide a copy of any statement of disagreement to the extent that disclosure accounting is maintained in accordance with 32 CFR 310.25 and shall advise the individual:

(i) Of the reason and authority for the denial.

(ii) Of his or her right to file a statement of the reason for disagreeing with the OSD/JS Privacy Office's decision.

(iii) Of the procedures for filing a statement of disagreement.

(iv) That the statement filed shall be made available to anyone the record is disclosed to, together with a brief statement by the WHS-Serviced Component summarizing its reasons for refusing to amend the records.

(10) If the Chief, OSD/JS Privacy Office, determines that the record should be amended in accordance with the individual's request, the WHS-Serviced Component shall amend the record, advise the individual, and inform previous recipients where a disclosure accounting has been maintained in accordance with 32 CFR 310.25.

(11) All appeals should be processed within 30 workdays after receipt by the proper office. If the Chief, OSD/JS Privacy Office, determines that a fair and equitable review cannot be made within that time, the individual shall be informed in writing of the reasons for the delay and of the approximate date the review is expected to be completed.

(g) *Disclosure of Disputed Information.*

(1) If the OSD/JS Privacy Office determines the record should not be amended and the individual has filed a statement of disagreement under paragraph (f)(8) of this section, the WHS-Serviced Component shall annotate the disputed record so it is apparent to any person to whom the record is disclosed that a statement has been filed. Where feasible, the notation itself shall be integral to the record. Where disclosure accounting has been made, the WHS-Serviced Component shall advise previous recipients that the record has been disputed and shall provide a copy of the individual's statement of disagreement in accordance with 32 CFR 310.21.

(i) This statement shall be maintained to permit ready retrieval whenever the disputed portion of the record is disclosed.

(ii) When information that is the subject of a statement of disagreement is subsequently disclosed, the WHS-Serviced Component designated official shall note which information is disputed and provide a copy of the individual's statement.

(2) The WHS-Serviced Component shall include a brief summary of its reasons for not making a correction

when disclosing disputed information. Such statement shall normally be limited to the reasons given to the individual for not amending the record.

(3) Copies of the WHS-Serviced Component summary will be treated as part of the individual's record; however, it will not be subject to the amendment procedure outlined in paragraph (f) of this section.

(h) *Penalties.* (1) *Civil Action.* An individual may file a civil suit against the WHS-Serviced Component or its employees if the individual feels certain provisions of the Privacy Act have been violated.

(2) *Criminal Action.* (i) Criminal penalties may be imposed against an officer or employee of a WHS-Serviced Component for these offenses listed in the Privacy Act:

(A) Willful unauthorized disclosure of protected information in the records;

(B) Failure to publish a notice of the existence of a record system in the FEDERAL REGISTER; and

(C) Requesting or gaining access to the individual's record under false pretenses.

(ii) An officer or employee of a WHS-Serviced Component may be fined up to \$5,000 for a violation as outlined in paragraphs (h)(2)(i)(A) through (h)(2)(i)(C) of this section.

(i) *Litigation Status Sheet.* Whenever a complaint citing the Privacy Act is filed in a U.S. District Court against the Department of Defense, a WHS-Serviced Component, or any employee of a WHS-Serviced Component, the responsible system manager shall promptly notify the OSD/JS Privacy Office, which shall notify the DPO. The litigation status sheet in appendix H of 32 CFR part 310 provides a standard format for this notification. (The initial litigation status sheet shall, as a minimum, provide the information required by items 1 through 6). A revised litigation status sheet shall be provided at each stage of the litigation. When a court renders a formal opinion or judgment, copies of the judgment or opinion shall be provided to the OSD/JS Privacy Office with the litigation status sheet reporting that judgment or opinion.

(j) *Computer Matching Programs.* 32 CFR 310.52 prescribes that all requests

§ 311.7

for participation in a matching program (either as a matching agency or a source agency) be submitted to the DPO for review and compliance. The WHS-Serviced Components shall submit a courtesy copy to the OSD/JS Privacy Office at the time of transmittal to the DPO.

§ 311.7 OSD/JS Privacy Office Processes.

The OSD/JS Privacy Office shall:

(a) Exercise oversight and administrative control of the OSD/JS Privacy Program for the WHS-Serviced Components.

(b) Provide guidance and training to the WHS-Serviced Components as required by 32 CFR 310.37.

(c) Collect and consolidate data from the WHS-Serviced Components and submit reports to the DPO, as required by 32 CFR 310.40 or otherwise requested by the DPO.

(d) Coordinate and consolidate information for reporting all record systems, as well as changes to approved systems, to the DPO for final processing to the Office of Management and Budget, the Congress, and the FEDERAL REGISTER, as required by 32 CFR part 310.

(e) In coordination with DPO, serve as the appellate authority for the WHS-Serviced Components when a requester appeals a denial for access as well as when a requester appeals a denial for amendment or initiates legal action to correct a record.

(f) Refer all matters about amendments of records and general and specific exemptions under 32 CFR 310.19, 310.28 and 310.29 to the proper WHS-Serviced Components.

§ 311.8 Procedures for exemptions.

(a) *General information.* The Secretary of Defense designates those Office of the Secretary of Defense (OSD) systems of records which will be exempt from certain provisions of the Privacy Act. There are two types of exemptions, general and specific. The general exemption authorizes the exemption of a system of records from all but a few requirements of the Act. The specific exemption authorizes exemption of a system of records or portion thereof, from only a few specific requirements.

32 CFR Ch. I (7-1-11 Edition)

If an OSD Component originates a new system of records for which it proposes an exemption, or if it proposes an additional or new exemption for an existing system of records, it shall submit the recommended exemption with the records system notice as outlined in § 311.6. No exemption of a system of records shall be considered automatic for all records in the system. The systems manager shall review each requested record and apply the exemptions only when this will serve significant and legitimate Government purpose.

(b) *General exemptions.* The general exemption provided by 5 U.S.C. 552a(j)(2) may be invoked for protection of systems of records maintained by law enforcement activities. Certain functional records of such activities are not subject to access provisions of the Privacy Act of 1974. Records identifying criminal offenders and alleged offenders consisting of identifying data and notations of arrests, the type and disposition of criminal charges, sentencing, confinement, release, parole, and probation status of individuals are protected from disclosure. Other records and reports compiled during criminal investigations, as well as any other records developed at any stage of the criminal law enforcement process from arrest to indictment through the final release from parole supervision are excluded from release.

(1) *System identifier and name:* DWHS P42.0, DPS Incident Reporting and Investigations Case Files.

(i) *Exemption.* Portions of this system that fall within 5 U.S.C. 552a(j)(2) are exempt from the following provisions of 5 U.S.C. 552a, Sections (c)(3) and (4); (d)(1) through (d)(5); (e)(1) through (e)(3); (e)(5); (f)(1) through (f)(5); (g)(1) through (g)(5); and (h) of the Act.

(ii) *Authority:* 5 U.S.C. 552a(j)(2).

(iii) *Reason:* The Defense Protective Service is the law enforcement body for the jurisdiction of the Pentagon and immediate environs. The nature of certain records created and maintained by the DPS requires exemption from access provisions of the Privacy Act of 1974. The general exemption, 5 U.S.C. 552a(j)(2), is invoked to protect ongoing

investigations and to protect from access criminal investigation information contained in this record system, so as not to jeopardize any subsequent judicial or administrative process taken as a result of information contained in the file.

(2) *System identifier and name:* JS006.CND, Department of Defense Counternarcotics C4I System.

(i) *Exemption:* Portions of this system that fall within 5 U.S.C. 552a(j)(2) are exempt from the following provisions of 5 U.S.C. 552a, section (c) (3) and (4); (d)(1) through (d)(5); (e)(1) through (e)(3); (e)(4)(G) and (e)(4)(H); (e)(5); (f)(1) through (f)(5); (g)(1) through (g)(5) of the Act.

(ii) *Authority:* 5 U.S.C. 552a(j)(2).

(iii) *Reason:* From subsection (c)(3) because the release of accounting of disclosure would inform a subject that he or she is under investigation. This information would provide considerable advantage to the subject in providing him or her with knowledge concerning the nature of the investigation and the coordinated investigative efforts and techniques employed by the cooperating agencies. This would greatly impede USSOUTHCOM's criminal law enforcement.

(iv) For subsections (c)(4) and (d) because notification would alert a subject to the fact that an investigation of that individual is taking place, and might weaken the on-going investigation, reveal investigatory techniques, and place confidential informants in jeopardy.

(v) From subsections (e)(4)(G) and (H) because this system of records is exempt from the access provisions of subsection (d) pursuant to subsection (j).

(vi) From subsection (f) because the agency's rules are inapplicable to those portions of the system that are exempt and would place the burden on the agency of either confirming or denying the existence of a record pertaining to a requesting individual might in itself provide an answer to that individual relating to an on-going criminal investigation. The conduct of a successful investigation leading to the indictment of a criminal offender precludes the applicability of established agency rules relating to verification of record, disclosure of the record to that individual,

and record amendment procedures for this record system.

(vii) For compatibility with the exemption claimed from subsection (f), the civil remedies provisions of subsection (g) must be suspended for this record system. Because of the nature of criminal investigations, standards of accuracy, relevance, timeliness and completeness cannot apply to this record system. Information gathered in criminal investigations is often fragmentary and leads relating to an individual in the context of one investigation may instead pertain to a second investigation.

(viii) From subsection (e)(1) because the nature of the criminal investigative function creates unique problems in prescribing a specific parameter in a particular case with respect to what information is relevant or necessary. Also, due to USSOUTHCOM's close liaison and working relationships with the other Federal, as well as state, local and foreign country law enforcement agencies, information may be received which may relate to a case under the investigative jurisdiction of another agency. The maintenance of this information may be necessary to provide leads for appropriate law enforcement purposes and to establish patterns of activity which may relate to the jurisdiction of other cooperating agencies.

(ix) From subsection (e)(2) because collecting information to the greatest extent possible directly from the subject individual may or may not be practicable in a criminal investigation. The individual may choose not to provide information and the law enforcement process will rely upon significant information about the subject from witnesses and informants.

(x) From subsection (e)(3) because supplying an individual with a form containing a Privacy Act Statement would tend to inhibit cooperation by many individuals involved in a criminal investigation. The effect would be somewhat inimical to established investigative methods and techniques.

(xi) From subsection (e)(5) because the requirement that records be maintained with attention to accuracy, relevance, timeliness, and completeness would unfairly hamper the criminal investigative process. It is the nature of

criminal law enforcement for investigations to uncover the commission of illegal acts at diverse stages. It is frequently impossible to determine initially what information is accurate, relevant, timely, and least of all complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significant as further investigation brings new details to light.

(xii) From subsection (e)(8) because the notice requirements of this provision could present a serious impediment to criminal law enforcement by revealing investigative techniques, procedures, and existence of confidential investigations.

(3)-(15) [Reserved]

(16) System identifier and name: DWHS E06, Enterprise Correspondence Control System (ECCS).

(i) *Exemption*: During the staffing and coordination of actions to, from, and within components in conduct of daily business, exempt materials from other systems of records may in turn become part of the case record in this document control system. To the extent that copies of exempt records from those "other" systems of records are entered into this system, the Office of the Secretary of Defense hereby claims the same exemptions for the records from those "other" systems that are entered into this system, as claimed for the original primary system of which they are a part.

(ii) *Authority*: 5 U.S.C. 552a (j)(2) and (k)(1) through (k)(7).

(iii) Records are only exempt from pertinent provisions of 5 U.S.C. 552a to the extent such provisions have been identified and an exemption claimed for the original record and the purposes underlying the exemption for the original record still pertain to the record which is now contained in this system of records. In general, the exemptions were claimed in order to protect properly classified information relating to national defense and foreign policy, to avoid interference during the conduct of criminal, civil, or administrative actions or investigations, to ensure protective services provided the President and others are not compromised, to protect the identity of confidential sources incident to Federal employ-

ment, military service, contract, and security clearance determinations, to preserve the confidentiality and integrity of Federal testing materials, and to safeguard evaluation materials used for military promotions when furnished by a confidential source. The exemption rule for the original records will identify the specific reasons why the records are exempt from specific provisions of 5 U.S.C. 552a.

(c) *Specific exemptions*. All systems of records maintained by any OSD Component shall be exempt from the requirements of 5 U.S.C. 552a(d) pursuant to subsection (k)(1) of that section to the extent that the system contains any information properly classified under Executive Order 11265, 'National Security Information,' dated June 28, 1979, as amended, and required by the Executive Order to be kept classified in the interest of national defense or foreign policy. This exemption, which may be applicable to parts of all systems of records, is necessary because certain record systems not otherwise specifically designated for exemptions may contain isolated information which has been properly classified. The Secretary of Defense has designated the following OSD system of records described below specifically exempted from the appropriate provisions of the Privacy Act pursuant to the designated authority contained therein:

(1) *System identifier and name*: DGC 16, Political Appointment Vetting Files.

(i) *Exemption*. Portions of this system of records that fall within the provisions of 5 U.S.C. 552a(k)(5) may be exempt from the following subsections (d)(1) through (d)(5).

(ii) *Authority*. 5 U.S.C. 552a(k)(5).

(iii) *Reasons*. From (d)(1) through (d)(5) because the agency is required to protect the confidentiality of sources who furnished information to the Government under an expressed promise of confidentiality or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. This confidentiality

is needed to maintain the Government's continued access to information from persons who otherwise might refuse to give it. This exemption is limited to disclosures that would reveal the identity of a confidential source.

(2) *System identifier and name:* DWHS P28, The Office of the Secretary of Defense Clearance File.

(i) *Exemption.* This system of records is exempt from subsections (c)(3) and (d) of 5 U.S.C. 552a, which would require the disclosure of investigatory material compiled solely for the purpose of determining access to classified information but only to the extent that disclosure of such material would reveal the identity of a source who furnished information to the Government under an expressed promise that the identity of the source would be held in confidence or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. A determination will be made at the time of the request for a record concerning the specific information which would reveal the identity of the source.

(ii) *Authority.* 5 U.S.C. 552a(k)(5).

(iii) *Reasons.* This exemption is required to protect the confidentiality of the sources of information compiled for the purpose of determining access to classified information. This confidentiality helps maintain the Government's continued access to information from persons who would otherwise refuse to give it.

(3) *System identifier and name:* DGC 04, Industrial Personnel Security Clearance Case Files.

(i) *Exemption.* All portions of this system which fall under 5 U.S.C. 552a(k)(5) are exempt from the following provisions of title 5 U.S.C. 552a: (c)(3); (d).

(ii) *Authority.* 5 U.S.C. 552a(k)(5).

(iii) *Reasons.* This system of records is exempt from subsections (c)(3) and (d) of section 552a of 5 U.S.C. which would require the disclosure of investigatory material compiled solely for the purpose of determining access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an expressed

promise that the identity of the source would be held in confidence, or prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. A determination will be made at the time of the request for a record concerning whether specific information would reveal the identity of a source. This exemption is required in order to protect the confidentiality of the sources of information compiled for the purpose of determining access to classified information. This confidentiality helps maintain the Government's continued access to information from persons who would otherwise refuse to give it.

(4) *System identifier and name:* DWHS P32, Standards of Conduct Inquiry File.

(i) *Exemption.* This system of records is exempted from subsections (c)(3) and (d) of 5 U.S.C. 552a, which would require the disclosure of: Investigatory material compiled for law enforcement purposes; or investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, or Federal contracts, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. If any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or otherwise be eligible, as a result of the maintenance of investigatory material compiled for law enforcement purposes, the material shall be provided to that individual, except to the extent that its disclosure would reveal the identity of a source who furnished information to the Government under an express promise or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. At the time of the request for a record, a determination will be made concerning whether a right, privilege, or benefit is denied or specific information would reveal the identity of a source.

(ii) *Authority.* 5 U.S.C. 552a(k)(2) and (5).

(iii) *Reasons.* These exemptions are necessary to protect the confidentiality of the records compiled for the purpose of: enforcement of the conflict of interest statutes by the Department of Defense Standards of Conduct Counselor, General Counsel, or their designees; and determining suitability, eligibility or qualifications for Federal civilian employment, military service, or Federal contracts of those alleged to have violated or caused others to violate the Standards of Conduct regulations of the Department of Defense.

(5) *System identifier and name:* DUSDP 02, Special Personnel Security Cases.

(i) *Exemption:* All portions of this system which fall under 5 U.S.C. 552a(k)(5) are exempt from the following provisions of 5 U.S.C. 552a: (c)(3); (d).

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

(iii) *Reasons:* This system of records is exempt from subsections (c)(3) and (d) of 5 U.S.C. 552a which would require the disclosure of investigatory material compiled solely for the purpose of determining access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an expressed promise that the identity of the source would be held in confidence or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. A determination will be made at the time of the request for a record concerning whether specific information would reveal the identity of a source. This exemption is required in order to protect the confidentiality of the sources of information compiled for the purpose of determining access to classified information. This confidentiality helps maintain the Government's continued access to information from persons who would otherwise refuse to give it.

(6) *System identifier and name:* DODDS 02.0, Educator Application Files.

(i) *Exemption.* All portions of this system which fall within 5 U.S.C. 552a(k)(5) may be exempt from the following provisions of 5 U.S.C. 552a: (c)(3); (d).

(ii) *Authority.* 5 U.S.C. 552a(k)(5).

(iii) *Reasons.* It is imperative that the confidential nature of evaluation and

investigatory material on teacher application files furnished the Department of Defense Dependent Schools (DoDDS) under promises of confidentiality be exempt from disclosure to the individual to insure the candid presentation of information necessary to make determinations involving applicants suitability for DoDDS teaching positions.

(7) *System identifier and name:* DGC 20, DoD Presidential Appointee Vetting File.

(i) *Exemption:* Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source. Portions of this system of records that may be exempt pursuant to 5 U.S.C. 552a(k)(5) are subsections (d)(1) through (d)(5).

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

(iii) *Reason:* From (d)(1) through (d)(5) because the agency is required to protect the confidentiality of sources who furnished information to the Government under an expressed promise of confidentiality or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. This confidentiality is needed to maintain the Government's continued access to information from persons who otherwise might refuse to give it.

(8) *System identifier and name:* DWHS P29, Personnel Security Adjudications File.

(i) *Exemption:* Portions of this system of records that fall within the provisions of 5 U.S.C. 552a(k)(5) may be exempt from the following subsections (d)(1) through (d)(5).

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

(iii) *Reasons.* From (d)(1) through (d)(5) because the agency is required to protect the confidentiality of sources who furnished information to the Government under an expressed promise of confidentiality or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. This confidentiality

is needed to maintain the Government's continued access to information from persons who otherwise might refuse to give it. This exemption is limited to disclosures that would reveal the identity of a confidential source. At the time of the request for a record, a determination will be made concerning whether a right, privilege, or benefit is denied or specific information would reveal the identity of a source.

(9) *System identifier and name:* JS004SECDIV, Joint Staff Security Clearance Files.

(i) *Exemption:* Portions of this system of records are exempt pursuant to the provisions of 5 U.S.C. 552a(k)(5) from subsections 5 U.S.C. 552a(d)(1) through (d)(5).

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

(iii) *Reasons:* From subsections (d)(1) through (d)(5) because the agency is required to protect the confidentiality of sources who furnished information to the Government under an expressed promise of confidentiality or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. This confidentiality is needed to maintain the Government's continued access to information from persons who otherwise might refuse to give it. This exemption is limited to disclosures that would reveal the identity of a confidential source. At the time of the request for a record, a determination will be made concerning whether a right, privilege, or benefit is denied or specific information would reveal the identity of a source.

(10) *System identifier and name:* DFMP 26, Vietnamese Commando Compensation Files.

(i) *Exemption:* Information classified under E.O. 12958, as implemented by DoD 5200.1-R, may be exempt pursuant to 5 U.S.C. 552a(k)(1).

(ii) *Authority:* 5 U.S.C. 552a(k)(1).

(iii) *Reasons:* From subsection 5 U.S.C. 552a(d) because granting access to information that is properly classified pursuant to E.O. 12958, as implemented by DoD 5200.1-R, may cause damage to the national security.

(11) *System identifier and name:* DUSP 11, POW/Missing Personnel Office Files.

(i) *Exemption:* Information classified under E.O. 12958, as implemented by DoD 5200.1-R, may be exempt pursuant to 5 U.S.C. 552a(k)(1).

(ii) *Authority:* 5 U.S.C. 552a(k)(1).

(iii) *Reasons:* From subsection 5 U.S.C. 552a(d) because granting access to information that is properly classified pursuant to E.O. 12958, as implemented by DoD 5200.1-R, may cause damage to the national security.

(12) *System identifier and name:* DFOISR 05, Freedom of Information Act Case Files.

(i) *Exemption:* During the processing of a Freedom of Information Act request, exempt materials from other systems of records may in turn become part of the case record in this system. To the extent that copies of exempt records from those 'other' systems of records are entered into this system, the Office of the Secretary of Defense claims the same exemptions for the records from those 'other' systems that are entered into this system, as claimed for the original primary system of which they are a part.

(ii) *Authority:* 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), (k)(3), (k)(4), (k)(5), (k)(6), and (k)(7).

(iii) *Reasons:* Records are only exempt from pertinent provisions of 5 U.S.C. 552a to the extent such provisions have been identified and an exemption claimed for the original record and the purposes underlying the exemption for the original record still pertain to the record which is now contained in this system of records. In general, the exemptions were claimed in order to protect properly classified information relating to national defense and foreign policy, to avoid interference during the conduct of criminal, civil, or administrative actions or investigations, to ensure protective services provided the President and others are not compromised, to protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations, to preserve the confidentiality and integrity of Federal testing materials, and to safeguard evaluation materials used for military promotions when furnished by a confidential source. The exemption rule for the original records will identify

§311.8

32 CFR Ch. I (7–1–11 Edition)

the specific reasons why the records are exempt from specific provisions of 5 U.S.C. 552a.

(13) *System identifier and name:* DFOISR 10, Privacy Act Case Files.

(i) *Exemption:* During the processing of a Privacy Act request (which may include access requests, amendment requests, and requests for review for initial denials of such requests), exempt materials from other systems of records may in turn become part of the case record in this system. To the extent that copies of exempt records from those ‘other’ systems of records are entered into this system, the Office of the Secretary of Defense hereby claims the same exemptions for the records from those ‘other’ systems that are entered into this system, as claimed for the original primary system of which they are a part.

(ii) *Authority:* 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), (k)(3), (k)(4), (k)(5), (k)(6), and (k)(7).

(iii) Records are only exempt from pertinent provisions of 5 U.S.C. 552a to the extent such provisions have been identified and an exemption claimed for the original record and the purposes underlying the exemption for the original record still pertain to the record which is now contained in this system of records. In general, the exemptions were claimed in order to protect properly classified information relating to national defense and foreign policy, to avoid interference during the conduct of criminal, civil, or administrative actions or investigations, to ensure protective services provided the President and others are not compromised, to protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations, to preserve the confidentiality and integrity of Federal testing materials, and to safeguard evaluation materials used for military promotions when furnished by a confidential source. The exemption rule for the original records will identify the specific reasons why the records are exempt from specific provisions of 5 U.S.C. 552a.

(14) *System identifier and name:* DHRA 02, PERSEREC Research Files.

(i) *Exemption:* (A) Investigative material compiled solely for the purpose of

determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(B) Therefore, portions of this system may be exempt pursuant to 5 U.S.C. 552a(k)(5) from the following subsections of 5 U.S.C. 552a(c)(3), (d), and (e)(1).

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

(iii) *Reasons:* (A) From subsection (c)(3) and (d) when access to accounting disclosures and access to or amendment of records would cause the identity of a confidential source to be revealed. Disclosure of the source’s identity not only will result in the Department breaching the promise of confidentiality made to the source, but it will impair the Department’s future ability to compile investigatory material for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access to classified information. Unless sources can be assured that a promise of confidentiality will be honored, they will be less likely to provide information considered essential to the Department in making the required determinations.

(B) From (e)(1) because in the collection of information for investigatory purposes, it is not always possible to determine the relevance and necessity of particular information in the early stages of the investigation. In some cases, it is only after the information is evaluated in light of other information that its relevance and necessity becomes clear. Such information permits more informed decisionmaking by the Department when making required suitability, eligibility, and qualification determinations.

(15) *System identifier and name:* DCIFA 01, CIFA Operational and Analytical Records.

(i) *Exemptions:* This system of records is a compilation of information from other Department of Defense and U.S. Government systems of records. To the extent that copies of exempt records from those ‘other’ systems of records

are entered into this system, OSD hereby claims the same exemptions for the records from those ‘other’ systems that are entered into this system, as claimed for the original primary system of which they are a part.

(ii) *Authority:* 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), (k)(3), (k)(4), (k)(5), (k)(6), and (k)(7).

(iii) Records are only exempt from pertinent provisions of 5 U.S.C. 552a to the extent (1) such provisions have been identified and an exemption claimed for the original record and (2) the purposes underlying the exemption for the original record still pertain to the record which is now contained in this system of records. In general, the exemptions are claimed in order to protect properly classified information relating to national defense and foreign policy, to avoid interference during the conduct of criminal, civil, or administrative actions or investigations, to ensure protective services provided the President and others are not compromised, to protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations, and to preserve the confidentiality and integrity of Federal evaluation materials. The exemption rule for the original records will identify the specific reasons why the records are exempt from specific provisions of 5 U.S.C. 552a.

(16)–(17) [Reserved]

(18) *System identifier and name:* DMDC 12 DoD, Joint Personnel Adjudication System (JPAS).

(i) *Exemption:* Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

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

(iii) *Reasons:* (A) from subsections (c)(3) and (d) when access to accounting disclosure and access to or amendment of records would cause the identity of a confidential source to be revealed. Disclosure of the source’s identity not only will result in the Department

breaching the promise of confidentiality made to the source but it will impair the Department’s future ability to compile investigatory material for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access to classified information. Unless sources can be assured that a promise of confidentiality will be honored, they will be less likely to provide information considered essential to the Department in making the required determinations.

(B) From subsection (e)(1) because in the collection of information for investigatory purposes, it is not always possible to determine the relevance and necessity of particular information in the early stages of the investigation. It is only after the information is evaluated in light of other information that its relevance and necessity becomes clear. Such information permits more informed decision-making by the Department when making required suitability, eligibility, and qualification determinations.

(19) *System identifier and name:* DA&M 01, Civil Liberties Program Case Management System.

(i) *Exemptions:* Records contained in this System of Records may be exempted from the requirements of subsections (c)(3); (d)(1), (2), (3), and (4); (e)(1) and (e)(4)(G), (H), and (I); and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1). Records may be exempted from these subsections or, additionally, from the requirements of subsections (c)(4); (e)(2), (3), and (8) of the Privacy Act of 1974 consistent with any exemptions claimed under 5 U.S.C. 552a (j)(2) or (k)(1), (k)(2), or (k)(5) by the originator of the record, provided the reason for the exemption remains valid and necessary. An exemption rule for this system has been promulgated in accordance with the requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c) and (e) and is published at 32 CFR part 311.

(ii) *Authority:* 5 U.S.C. 552a (j)(2), (k)(1), (k)(2), or (k)(5).

(iii) *Reasons:* (A) From subsections (c)(3) (accounting of disclosures) because an accounting of disclosures from records concerning the record subject would specifically reveal an intelligence or investigative interest on

the part of the Department of Defense and could result in release of properly classified national security or foreign policy information.

(B) From subsections (d)(1), (2), (3) and (4) (record subject's right to access and amend records) because affording access and amendment rights could alert the record subject to the investigative interest of law enforcement agencies or compromise sensitive information classified in the interest of national security. In the absence of a national security basis for exemption, records in this system may be exempted from access and amendment to the extent necessary to honor promises of confidentiality to persons providing information concerning a candidate for position. Inability to maintain such confidentiality would restrict the free flow of information vital to a determination of a candidate's qualifications and suitability.

(C) From subsection (e)(1) (maintain only relevant and necessary records) because in the collection of information for investigatory purposes, it is not always possible to determine the relevance and necessity of particular information in the early stages of the investigation. It is only after the information is evaluated in light of other information that its relevance and necessity becomes clear. In the absence of a national security basis for exemption under subsection (k)(1), records in this system may be exempted from the relevance requirement pursuant to subsection (k)(5) because it is not possible to determine in advance what exact information may assist in determining the qualifications and suitability of a candidate for position. Seemingly irrelevant details, when combined with other data, can provide a useful composite for determining whether a candidate should be appointed.

(D) From subsections (e)(4)(G) and (H) (publication of procedures for notifying subject of the existence of records about them and how they may access records and contest contents) because the system is exempted from subsection (d) provisions regarding access and amendment, and from the subsection (f) requirement to promulgate agency rules. Nevertheless, the Office of the Secretary of Defense has pub-

lished notice concerning notification, access, and contest procedures because it may, in certain circumstances, determine it appropriate to provide subjects access to all or a portion of the records about them in this system of records.

(E) From subsection (e)(4)(I) (identifying sources of records in the system of records) because identifying sources could result in disclosure of properly classified national defense or foreign policy information, intelligence sources and methods, and investigatory techniques and procedures. Notwithstanding its proposed exemption from this requirement the Office of the Secretary of Defense identifies record sources in broad categories sufficient to provide general notice of the origins of the information it maintains in this system of records.

(F) From subsection (f) (agency rules for notifying subjects to the existence of records about them, for accessing and amending records, and for assessing fees) because the system is exempt from subsection (d) provisions regarding access and amendment of records by record subjects. Nevertheless, the Office of the Secretary of Defense has published agency rules concerning notification of a subject in response to his request if any system of records named by the subject contains a record pertaining to him and procedures by which the subject may access or amend the records. Notwithstanding exemption, the Office of the Secretary of Defense may determine it appropriate to satisfy a record subject's access request.

[74 FR 58205, Nov. 12, 2009, as amended at 74 FR 55778, Oct. 29, 2009; 76 FR 22612, Apr. 22, 2011]

PART 312—OFFICE OF THE INSPECTOR GENERAL (OIG) PRIVACY PROGRAM

Sec.	
312.1	Purpose.
312.2	Definitions.
312.3	Procedure for requesting information.
312.4	Requirements for identification.
312.5	Access by subject individuals.
312.6	Fees.
312.7	Request for correction or amendment.
312.8	OIG review of request for amendment.
312.9	Appeal of initial amendment decision.