

DSS decision not to amend a record is received from the subject individual, prior recipients of the record identified in disclosure accountings will be notified to the extent possible. In some cases, prior recipients cannot be located due to reorganization or deactivations. In these cases, the personnel security element of the receiving Defense Component will be sent the notification or statement for appropriate action.

(i) *Ownership of DSS Investigative Records.* Personnel security investigative reports shall not be retained by DoD recipient organizations. Such reports are considered to be the property of the investigating organization and are on loan to the recipient organization for the purpose for which requested. All copies of such reports shall be destroyed within 120 days after the completion of the final personnel security determination and the completion of all personnel action necessary to implement the determination. Reports that are required for longer periods may be retained only with the specific written approval of the investigative organization.

(j) *Consultation and referral.* DSS system of records may contain records originated by other components or agencies which may have claimed exemptions for them under the Privacy Act of 1974. When any action that may be exempted is initiated concerning such a record, consultation with the originating agency or component will be effected. Where appropriate such records will be referred to the originating component or agency for approval or disapproval of the action.

**PART 322—NATIONAL SECURITY
AGENCY/CENTRAL SECURITY
SERVICES PRIVACY ACT
PROGRAM**

- Sec.
322.1 Purpose and applicability.
322.2 Definitions.
322.3 Policy.
322.4 Responsibilities.
322.5 Procedures.
322.6 Establishing exemptions.
322.7 Exempt systems of records.

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

SOURCE: 68 FR 28757, May 27, 2003, unless otherwise noted.

§ 322.1 Purpose and applicability.

(a) This part implements the Privacy Act of 1974 (5 U.S.C. 552a), as amended and the Department of Defense Privacy Program (32 CFR part 310) within the National Security Agency/Central Security Service (NSA/CSS); establishes policy for the collection and disclosure of personal information about individuals; assigns responsibilities and establishes procedures for collecting personal information and responding to first party requests for access to records, amendments of those records, or an accounting of disclosures.

(b) This part applies to all NSA/CSS elements, field activities and personnel and governs the release or denial of any information under the terms of the Privacy Act of 1974 (5 U.S.C. 552a), as amended.

§ 322.2 Definitions.

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

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

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

Employees of NSA/CSS. Individuals employed by, assigned or detailed to the NSA/CSS. This part also applies to NSA/CSS contractor personnel who administer NSA/CSS systems of records that are subject to the Privacy Act.

FOIA Request. A written request for NSA/CSS records, made by any person, that either explicitly or implicitly invokes the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended. FOIA requests will be accepted by U.S. mail

or its equivalent, facsimile, or the Internet, or employees of NSA/CSS may hand deliver them.

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

Maintain. Includes maintain, collect, use or disseminate.

Medical Records. Documents relating to the physical care and treatment of an individual.

Privacy Act Request. A written request containing a signature submitted by a U.S. citizen or alien admitted for permanent residence for access to or amendment of records on himself/herself which are contained in a PA system of records. PA requests will be accepted via mail or facsimile, or NSA/CSS employees may hand deliver them. Digital signatures will be accepted via the Internet by October 21, 2003. Until then, PA requests will not be accepted via the Internet. Requests received via the Internet will not be acknowledged. Regardless of whether the requester cites the FOIA, PA, or no law, the request for records will be processed under both this part and the FOIA. Requests for amendments will be processed pursuant to the PA.

Personal information. The collection of two or more pieces of information that is about an individual: *e.g.* name and date of birth, Social Security Number.

Personal notes. Notations created in paper or electronic form for the convenience and at the discretion of the originator, for the originator's eyes only, and over which NSA/CSS exercises no control. Personal notes are not agency records within the meaning of the Privacy Act (PA) or the Freedom of Information Act (FOIA). However, once the personal note, or information contained therein, is shared with another individual, it becomes an Agency record and is subject to the provisions of the FOIA and, if appropriate, the PA.

Psychological Records. Documents relating to the psychological care and treatment of an individual.

Record. Any item, collection, or grouping of information, whatever the storage media (paper, electronic, etc.) about an individual or his or her education, financial transactions, medical history, criminal or employment history, and that contains his or her name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint, voice print, or a photograph. The record must be in existence and under the control of NSA/CSS at the time a request is made.

Routine use. The disclosure of a record outside NSA/CSS or the DoD for a use that is compatible with the purpose for which the information was collected and maintained by NSA/CSS. The routine use must be included in the published system of records.

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

§ 322.3 Policy.

(a) The National Security Agency/Central Security Service shall maintain in its records only such information about an individual that is relevant and necessary to accomplish a purpose of the Agency, and that is required or authorized to be maintained by statute or Executive Order. Information about an individual shall, to the greatest extent practicable, be collected directly from the individual if the information may result in adverse determinations about the individual's rights, benefits, and privileges under any Federal program. Records used by this Agency in making adverse determinations about an individual shall be maintained with such accuracy, relevance, timeliness and completeness as is reasonably necessary to assure fairness to the individual. The Agency shall protect the privacy of individuals identified in its records, and shall permit an individual to request access to personal information in records on

§ 322.4

32 CFR Ch. I (7-1-03 Edition)

himself/herself and to request correction or amendment of factual information contained in such records. These policies are consistent with the spirit and intent of the PA, and are subject to exemptions under the Act, as defined in § 322.7, and legal requirements to protect sensitive NSA information such as the intelligence sources and methods the Agency employs to fulfill its mission.

(b) Pursuant to written requests submitted in accordance with the PA, the NSA/CSS shall make records available consistent with the Act and the need to protect government interests pursuant to subsections (d) and (k) of the Privacy Act. Oral requests for information shall not be accepted. Before the Agency responds to a request, the request must comply with the provisions of this part.

(c) In order that members of the public have timely access to unclassified information regarding NSA activities, requests for information that would not be withheld if requested under the FOIA or the PA may be honored through appropriate means without requiring the requester to invoke the FOIA or the PA. Although a record may require minimal redaction before its release, this fact alone shall not require the Agency to direct the requester to submit a formal FOIA or PA request for the record.

§ 322.4 Responsibilities.

(a) The Director's Chief of Staff (DC) is responsible for overseeing the administration of the PA. The Director of Policy (DC3), or the Deputy Director of Policy, if so designated, shall carry out this responsibility on behalf of the Chief of Staff and shall:

(1) Provide policy guidance to NSA/CSS on PA issues.

(2) Provide policy guidance to PA coordinators for processing PA requests from NSA/CSS employees who will be using the records within NSA/CSS spaces.

(3) Provide training of NSA/CSS employees and contractors in the requirements of the PA. Specialized training is provided to special investigators and employees who deal with the news media or the public.

(4) Receive, process, and respond to PA requests from individuals and employees who require the information for use outside of NSA/CSS spaces.

(i) Conduct the appropriate search for and review of records.

(ii) Provide the requester with copies of all releasable material.

(iii) Notify the requester of any adverse determination, including his/her right to appeal an adverse determination to the NSA/CSS Appeal Authority.

(iv) Assure the timeliness of responses.

(5) Receive, process and respond to PA amendment requests to include:

(i) Obtain comments and supporting documentation from the organization originating the record.

(ii) Conduct a review of all documentation relevant to the request.

(iii) Advise the requester of the Agency's decision.

(iv) Notify the requester of any adverse determination, including his/her right to appeal the adverse determination to the NSA/CSS Appeal Authority.

(v) Direct the appropriate Agency organization to amend a record and advise other record holders to amend the record when a decision is made in favor of a requester.

(vi) Assure the timeliness of responses.

(6) Ensure that Agency employees (internal requesters) that have access to NSA/CSS spaces are given access to all or part of a PA record to which the employee was denied by the record holder when, after a review of the circumstances by the Director of Policy, it is determined that access should be granted. For those individuals who do not have access to NSA/CSS spaces see § 322.6 of this part.

(7) Conduct Agency reviews in accordance with OMB Circular A-130¹ and 32 CFR part 310.

(8) Deposit in the U.S. Treasury all fees collected as a result of charges levied for the duplication of records provided under the PA and maintain the necessary accounting records for such fees.

¹Available from <http://www.whitehouse.gov/omb/circulars/index.html>.

Office of the Secretary of Defense

§ 322.4

(b) The NSA/CSS Privacy Act Appeal Authority is designated as the reviewing authority for requests for review of denials by the Director of Policy to provide access to a record and/or to amend a record. The PA Appeal Authority is the Deputy Director, NSA. In the absence of the Deputy Director, the Director's Chief of Staff serves as the Appeal Authority.

(c) The General Counsel (GC) or his designee shall:

(1) Advise on all legal matters concerning the PA.

(2) Advise the Director of Policy and other NSA/CSS organizations, as appropriate, of legal decisions including rulings by the Justice Department and actions by the DoD Privacy Board involving the PA.

(3) Review proposed responses to PA requests to ensure legal sufficiency, as appropriate.

(4) Provide a legal review of proposed Privacy Act notices and amendments for submission to the Defense Privacy Office.

(5) Assist, as required, in the preparation of PA reports for the Department of Defense and other authorities.

(6) Review proposals to collect PA information for legal sufficiency, assist in the development of PA statements and warning statements when required and approve prior to use.

(7) Represent the Agency in all judicial actions related to the PA by providing support to the Department of Justice and by keeping the DoD Office of General Counsel apprised of pending PA litigation. A litigation status sheet will be provided to the Defense Privacy Office.

(8) Assist in the education of new and current employees, including contractors, to the requirements of the PA.

(9) Review PA and PA Amendment appeals, prepare responses, and submit them to the NSA/CSS Appeal Authority for final decision.

(10) Notify the Director of Policy of the outcome of all appeals.

(d) The Associate Director for Human Resources Services or designee shall:

(1) Establish the physical security requirements for the protection of personal information and ensure that such requirements are maintained.

(2) Establish and ensure compliance with procedures governing the pledging of confidentiality to sources of information interviewed in connection with inquiries to determine suitability, eligibility or qualifications for Federal employment, Federal contracts, or access to classified information.

(3) Retain copies of records processed pursuant to the PA. The retention schedule is six years from the date records were provided to the requester if deletions were made and two years if records were provided in their entirety.

(4) Ensure the prompt delivery of all PA requests to the Director of Policy.

(5) Ensure the prompt delivery of all Privacy Act appeals of an adverse determination to the NSA/CSS PA Appeal Authority staff.

(6) Ensure that forms used to collect PA information meet the requirements of the PA.

(7) Compile, when required, estimates of cost incurred in the preparation or modification of forms requiring PA Statements.

(8) Assist in the development of training courses to educate new and current Agency employees, including contractors, of the provisions of the PA.

(9) Respond to PA requests for access to records, as appropriate.

(10) Establish procedures for the protection of personal information and ensure compliance with the procedures.

(e) The Inspector General (IG) shall:

(1) Be alert to Privacy Act compliance and to managerial administrative, and operational problems associated with the implementation of this part and document any such problems and remedial actions, if any, in official reports to responsible Agency officials, when appropriate.

(2) Respond, as appropriate, to PA requests.

(3) Establish procedures for the protection of personal records under the control or in the possession of OIG and ensure compliance with the procedures.

(f) Chiefs of Directorates, Associate Directorates, and Field Elements shall:

(1) Ensure that no systems or subsets of Systems of Records other than those published in the FEDERAL REGISTER are maintained within their components or field elements.

§ 322.4

32 CFR Ch. I (7-1-03 Edition)

(2) Establish rules of conduct for persons who design, use or maintain Systems of Records within their components or field elements and ensure compliance with these rules.

(3) Establish, in consultation with the Associate Director of Human Resources or designee, the physical security requirements for the protection of personal information and ensure that such requirements are maintained.

(4) Ensure that no records are maintained within their components or field elements which describe how any individual exercises rights guaranteed by the First Amendment to the Constitution of the United States unless expressly authorized by statute, or by the individual about whom the record is maintained, or unless pertinent to, and within the scope of, an authorized law enforcement activity.

(5) Ensure that records contained in the Systems of Records within their components or field elements are not disclosed to anyone other than in conformance with the Privacy Act, to include the routine uses for such records published in the FEDERAL REGISTER.

(6) Maintain only such information about an individual as is relevant and necessary to accomplish a purpose of the Agency required to be accomplished by statute and Executive Order.

(7) Maintain all records which are used by the Agency in making any determination about any individual with such accuracy, relevancy, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual in any determination.

(8) Establish procedures for protecting the confidentiality of personal records maintained or processed by computer systems and ensure compliance with the procedures.

(9) Designate a primary and alternate PA coordinator to be responsible for PA matters and inform the Office of Policy of the designations. Subordinate PA coordinators may be appointed at office level.

(10) Ensure that the Privacy Act coordinators acquire the necessary training in the theory and administration of the Privacy Act.

(11) Ensure that the Privacy Act coordinators conduct, to the extent practicable, on-the-job PA training of su-

pervisors and records handlers in their organizations.

(12) Respond to PA requests to review records, as appropriate.

(13) Establish procedures for the protection of personal records and ensure compliance with the procedures.

(14) Establish procedures to ensure that requests for copies of PA records needed for external use, outside of NSA/CSS, shall be delivered to the Director of Policy immediately upon receipt once the request is identified as a Privacy Act request or appears to be intended as such a request.

(15) Publish, as necessary, internal PA procedures which are consistent with the Privacy Act and this part.

(16) Maintain an accounting of disclosures of records as described in §322.5 of this part.

(17) Coordinate with the Office of the General Counsel any proposed new record systems or changes (either alterations or amendments) to existing systems. Notice of new record systems or alterations to existing systems must be published in the FEDERAL REGISTER at least 30 days and Congress and the Office of Management and Budget must be given 40 days to review the new/altere d system before implementation.

(18) Collect and forward to the Director of Policy information necessary to prepare reports, as requested.

(19) Respond promptly to the Director of Policy and the PA Appeal Authority decisions concerning the granting access to records, amending records, or filing statements of disagreements.

(20) Ensure that forms (paper or electronic) used to collect PA information meet the requirements of the PA.

(21) Establish procedures to ensure that requests to conduct computer matching are forwarded to the Director of Policy.

(g) Each field element shall designate a Privacy Act (PA) Coordinator to ensure compliance with this part and to receive and, where appropriate, process PA requests. Section 322.6 of this part describes the procedure for individuals to gain access to records and the responsibilities of the PA Coordinators. Consistent with the provisions of 32 CFR parts 285 and 286 and 32 CFR part

310 special procedures apply to the disclosure of certain medical records and psychological records. Field elements should consult the PA Coordinator of the Office of Occupational Health, Environment and Safety Services before disclosing such information. (See paragraph (d)(9) of this section.)

(h) All NSA/CSS organizations and field elements responsible for electronic/paper forms or other methods used to collect personal information from individuals shall determine, with General Counsel's concurrence, which of those forms or methods require Privacy Act Statements and shall prepare the required statements. The Office of Policy requires all organizations or elements using such forms or methods shall ensure that respondents read, understand, and sign the statements before supplying the requested information. In addition, organizations must obtain the Director of Policy and the Office of General Counsel approval prior to the collection of personal information in electronic format.

§ 322.5 Procedures.

(a) The Director of Policy, or the Deputy Director of Policy, if so designated, shall provide guidance to Privacy Act Coordinators for processing requests and releasing NSA/CSS information within the confines of the NSA/CSS. If any organization or element believes a request to review a PA record should be denied, it shall advise the requester of the procedures for requesting a review of the circumstances of the case by the Director of Policy.

(b) Persons Authorized Access to NSA/CSS Facilities: (1) Requests from NSA/CSS affiliates with authorized access to NSA/CSS facilities to review and/or obtain a copy of PA records in a Systems of Records for use within NSA/CSS spaces or for the inspection of an accounting of disclosures of the record shall be in writing, using the Privacy Act Information Request form. Requests shall normally be submitted directly to the Privacy Act Coordinator in the office holding the record. In the case of requests for access to records maintained in the individual's own organization, the Privacy Act Coordinator for that organization shall direct the requester to the person or of-

fice holding the record. A Privacy Act Information Request form shall be submitted to the holder of each record desired. The Privacy Act Coordinator shall assist supervisors and record handlers in processing the request and shall maintain an accounting for reporting purposes. Individuals shall not be permitted to review or obtain an internal copy of IG, OGC and/or certain security records. The Personnel File, which was available upon request prior to the implementation of the Privacy Act, shall continue to be available for review without citing the Privacy Act or using the Privacy Act Information Request form.

(2) Requests to obtain a copy of PA records for use outside of NSA/CSS shall be forwarded to the Director of Policy, FOIA/PA Services (DC321) using the Privacy Act Information Request form or in any written format and must contain the individual's full name, signature, social security number, description of the records sought and a work or home phone number. Requests shall be processed pursuant to the Privacy Act and the FOIA.

(c) Persons Not Authorized Access to NSA/CSS Facilities: (1) Requests from individuals who do not have authorized access to NSA/CSS facilities must be in writing, contain the individual's full name, current address, signature, social security number and a description of the records sought. The mailing address for the FOIA/PA office is: National Security Agency, ATTN: FOIA/PA Services (DC321), 9800 Savage Road, Suite 6248, Ft. George G. Meade, MD 20755-6248.

(2) FOIA/PA Services may, at its discretion, require an unsworn declaration or a notarized statement of identity. In accordance with 28 U.S.C. 1746, the language for an unsworn declaration is as follows:

(i) If executed without the United States: 'I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)'.

(ii) If executed within the United States, its territories, possessions, or commonwealths: 'I declare (or certify,

verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)'.

(d) General provisions regarding access and processing procedures: (1) The requester need not state a reason or otherwise justify the request. If the requester wishes to be accompanied by another person, the individual may be required to furnish a statement authorizing discussion or disclosure of the records in the presence of the other individual. If the requester wishes another person to obtain the records on his/her behalf, the requester shall provide a written statement appointing that person as his/her representative, authorizing that individual access to the records and affirming that such access shall not constitute an invasion of the requester's privacy or a violation of his/her rights under the Privacy Act. In addition, requests from parents or legal guardians for records on a minor may be accepted providing the individual is acting on behalf of the minor and evidence is provided to support his or her parentage (birth certificate showing requester as a parent) or guardianship (a court order establishing guardianship).

(2) The Director of Policy and FOIA/PA Services (DC321) shall endeavor to respond to a direct request to the NSA/CSS within 20 working days of receipt. In the event the FOIA/PA Services cannot respond within 20 working days due to unusual circumstances, the requester shall be advised of the reason for the delay and negotiate a completion date with the requester. Direct requests to NSA/CSS shall be processed in the order in which they are received. Requests referred to NSA/CSS by other government agencies shall be placed in the processing queue according to the date the requester's letter was received by the referring agency, if that date is known. If it is not known, it shall be placed in the appropriate processing queue according to the date of the requester's letter.

(3) FOIA/PA requests for copies of records shall be worked in chronological order within six queues ("super easy," "sensitive/personal easy," "non-personal easy," "sensitive/personal voluminous," "non-personal complex,"

and "expedite"). The processing queues are defined as follows:

(i) *Super Easy Queue*—The super easy queue is for requests for which no responsive records are located or for material that requires minimal specialized review.

(ii) *Sensitive/Personal Easy Queue*—The sensitive/personal easy queue contains FOIA and PA records that contain sensitive personal information, typically relating to the requester or requester's relatives, and that do not require a lengthy review. DC321 staff members who specialize in handling sensitive personal information process these requests.

(iii) *Non-Personal Easy Queue*—The non-personal easy queue contains all other types of NSA records not relating to the requester, that often contain classified information that may require coordinated review among NSA components, and that do not require a lengthy review. DC321 staff members who specialize in complex classification issues process these requests.

(iv) *Sensitive/Personal Voluminous Queue*—The sensitive/personal voluminous queue contains FOIA and PA records that contain sensitive personal information, typically relating to the requester or requester's relatives, and that require a lengthy review because of the high volume of responsive records. These records may also contain classified information that may require coordinated review in several NSA components. DC321 staff members who specialize in handling sensitive personal information process these requests.

(v) *Non-Personal Complex Queue*—The non-personal complex queue contains FOIA records not relating to the requester that require a lengthy review because of the high volume and/or complexity of responsive records. These records contain classified, often technical information that requires coordinated review among many specialized NSA components, as well as consultation with other government agencies. DC321 staff members who specialize in complex classification issues process these requests.

(vi) *Expedite Queue*—Cases meeting the criteria for expeditious processing

as defined in this section will be processed in turn within that queue by the appropriate processing team.

(4) Requesters shall be informed immediately if no responsive records are located. Following a search for and retrieval of responsive material, the initial processing team shall determine which queue in which to place the material, based on the criteria above, and shall so advise the requester. If the material requires minimal specialized review (super easy), the initial processing team shall review, redact if required, and provide the non-exempt responsive material to the requester immediately. The appropriate specialized processing team on a first in, first out basis within its queue shall process all other material. These procedures are followed so that a requester will not be required to wait a long period of time to learn that the Agency has no records responsive to his request or to obtain records that require minimal review.

(5) Requests for expeditious processing must include justification and a statement certifying that the information is true and correct to the best of the requester's knowledge. Expedited processing shall be granted if the requester demonstrates a compelling need for the information. Compelling need is defined as the failure to obtain the records on an expedited basis could reasonably be expected to pose an imminent threat to the life or physical safety of an individual or there would be an imminent loss of substantial due process rights.

(6) A request for expedited handling shall be responded to within 10 calendar days of receipt. The requester shall be notified whether his/her request meets the criteria for expedited processing within that time frame. If a request for expedited processing has been granted, a substantive response shall be provided within 20 working days of the date of the expedited decision. If a substantive response cannot be provided within 20 working days, a response shall be provided as soon as practicable and the chief of FOIA/PA Services shall attempt to negotiate an acceptable completion date with the requester, taking into account the number of cases preceding it in the ex-

pedite queue and the volume or complexity of the responsive material.

(7) Upon receipt of a request, FOIA/PA Services (DC321) shall review the request and direct the appropriate PA coordinator to search for responsive records. If the search locates the requested records, the PA coordinator shall furnish copies of the responsive documents to the FOIA/PA office that in turn shall make a determination as to the releasability of the records. All releasable records, or portions thereof, shall be provided to the requester. However, if information is exempt pursuant to the FOIA and PA, the requester shall be advised of the statutory basis for the denial of the information and the procedure for filing an appeal. In the instance where no responsive records are located, the requester shall be advised of the negative results and his/her right to appeal what could be considered an adverse determination. NSA does not have the authority to release another agency's information; therefore, information originated by another government agency shall be referred to the originating agency for its direct response to the requester or for review and return to NSA for response to the requester. The requester shall be advised that a referral has been made, except when notification would reveal exempt information.

(8) The requester shall not be charged a fee for the making of a comprehensible copy to satisfy the request for a copy of the documents. The requester may be charged for duplicate copies of the documents. However, if the direct cost of the duplicate copy is less than \$25.00, the fee shall be waived. Duplicating fees shall be assessed according to the following schedule: Office Copy \$.15 per page, Microfiche \$.25 per page, and Printed Material \$.02 per page. All payments shall be made by certified check or money order made payable to the Treasurer of the United States.

(9) A medical/psychological record shall normally be disclosed to the individual to whom it pertains. However, and consistent with 5 U.S.C. 552a(f)(3) of the Privacy Act, if in the judgment of an authorized Agency physician, the release of such information could have an adverse effect on the individual, the

individual shall be advised that it is in his best interest to receive the records through a physician of the requester's choice or, in the case of psychological records, through a licensed Psychiatrist or licensed Clinical Psychologist of the requester's choice. NSA/CSS may require certification that the individual is licensed to practice the appropriate specialty. Although the requester shall pay any fees charged by the physician or psychologist, NSA/CSS encourages individuals to take advantage of receiving their records through this means. If, however, the individual wishes to waive receiving the records through this means, the records shall be sent directly to the individual.

(10) Recipients of requests from NSA/CSS employees and affiliates for access to records within the confines of the NSA/CSS campus shall acknowledge the request within 10 working days of receipt, and access should be provided within 20 working days. If, for good cause, access cannot be provided within that time, the requester shall be advised in writing as to the reason and shall be given a date by which it is expected that access can be provided. If an office denies a request for access to a record, or any portion thereof, it shall notify the requester of its refusal and the reasons for it and shall advise the individual of the procedures for requesting a review of the circumstances by the Director of Policy. If the Director of Policy denies a request for access to a record or any portion thereof, the requester shall be notified of the refusal and the reasons the information was denied. The Director of Policy shall also advise the requester of the procedure for appealing to the NSA/CSS Privacy Act Appeal Authority. (See paragraph (e) of this section).

(11) Although classified portions of NSA/CSS records are exempt from disclosure pursuant to exemption (k)(1) of the Privacy Act and exemption (b)(1) of the FOIA, NSA, in its sole discretion, may choose to provide an NSA affiliate access to the classified portions of records about the affiliate if the affiliate possesses the requisite security clearance, special access approvals, and appropriate need-to-know for the classified information at issue. Classified

records may only be accessed by fully cleared personnel in NSA/CSS spaces. Disclosure of classified records under this provision shall not operate as a waiver of PA exemption (k)(1), FOIA exemption (b)(1), or of any other exemption or privilege that would otherwise authorize the Agency to withhold the classified records from disclosure. NSA's determination regarding an affiliate's need-to-know is not subject to appeal under this or any other authority. All copies of classified records made available to an NSA affiliate under the procedures of this Part shall carry the following statement: "This classified material is provided to you under the provisions of the Privacy Act of 1974. Furnishing you this material does not relieve you of your obligations under the laws of the United States (See, e.g., section 798 of Title 18, U.S. Code) to protect classified information. You may retain this material under proper protection as specified in the NSA/CSS Classification Manual; you may not remove it from NSA/CSS facilities."

(12) The procedures described in this part do not entitle an individual to have access to any information compiled in reasonable anticipation of a civil action or proceeding, nor do they require that a record be created.

(13) Requesting or obtaining access to records under false pretenses is a violation of the Privacy Act and is subject to criminal penalties.

(e) Appeal of Denial of an Adverse Determination: (1) Any individual advised of an adverse determination shall be notified of the right to appeal the initial decision within 60 calendar days of the date of the response letter and that the appeal must be addressed to the NSA/CSS FOIA/PA Appeal Authority, National Security Agency, 9800 Savage Road, Suite 6248, Fort George G. Meade, MD 20755-6248. The following actions are considered adverse determinations:

- (i) Denial of records or portions of records.
- (ii) Inability of NSA/CSS to locate responsive records.
- (iii) Denial of a request for expedited treatment.
- (iv) Non-agreement regarding completion date of request.

(v) The appeal shall reference the initial denial of access and shall contain, in sufficient detail and particularity, the grounds upon which the requester believes the appeal should be granted.

(2) The GC or his/her designee shall process appeals and make a recommendation to the Appeal Authority:

(i) Upon receipt of an appeal regarding the denial of information or the inability of the Agency to locate records on an individual, the GC or his/her designee shall provide a legal review of the denial and/or the adequacy of the search for responsive material, and make other recommendations as appropriate.

(ii) If the Appeal Authority determines that additional information may be released, the information shall be made available to the requester within 20 working days from receipt of the appeal. The conditions for responding to an appeal for which expedited treatment is sought by the requester are the same as those for expedited treatment on the initial processing of a request.

(iii) If the Appeal Authority determines that the denial was proper, the requester must be advised 20 days after receipt of the appeal that the appeal is denied. The requester likewise shall be advised of the basis for the denial and the provisions for judicial review of the Agency's appellate determination.

(iv) If a new search for records is conducted and produces additional records, the additional material shall be forwarded to the Director of Policy, as the initial denial authority (IDA), for review. Following review, the Director of Policy shall return the material to the GC with its recommendation for release or withholding. The GC will provide a legal review of the material, and the Appeal Authority shall make the release determination. Upon denial or release of additional information, the Appeal Authority shall advise the requester that more material was located and that the IDA and the Appeal Authority each conducted an independent review of the documents. In the case of denial, the requester shall be advised of the basis of the denial and the right to seek judicial review of the Agency's action.

(v) When a requester appeals the absence of a response to a request within

the statutory time limits, the GC shall process the absence of a response as it would denial of access to records. The Appeal authority shall advise the requester of the right to seek judicial review.

(vi) Appeals shall be processed using the same multi-track system as initial requests. If an appeal cannot be responded to within 20 days, the requirement to obtain an extension from the requester is the same as with initial requests. The time to respond to an appeal, however, may be extended by the number of working days (not to exceed 10) that were not used as additional time for responding to the initial request. That is, if the initial request is processed within 20 days so that the extra 10 days of processing which an agency can negotiate with the requester are not used, the response to the appeal may be delayed for that 10 days (or any unused portion of the 10 days).

(f) Amendment of Records:

(1) Minor factual errors may be corrected without resort to the Privacy Act or the provisions of this part, provided the requester and record holder agree to that procedure. Whenever possible, a copy of the corrected record should be provided to the requester.

(2) Requests for substantive changes to include deletions, removal of records, and amendment of significant factual information, because the information is incorrect or incomplete, shall be processed under the Privacy Act and the provisions of this part. The PA amendment process is limited to correcting records that are not accurate (factually correct), relevant, timely or complete.

(3) The amendment process is not intended to replace other existing NSA/CSS Agency procedures such as those for registering grievances or appealing performance appraisal ratings. Also, since the amendment process is limited to correcting factual information, it may not be used to challenge official judgments, such as performance ratings, promotion potential, and performance appraisals as well as subjective judgments made by supervisors, which reflect his/her observations and evaluations.

§ 322.5

32 CFR Ch. I (7-1-03 Edition)

(4) Requests for amendments must be in writing, include the individual's name, signature, a copy of the record under dispute or sufficient identifying particulars to permit timely retrieval of the affected record, a description of the information under dispute and evidence to support the amendment request. The mailing address for the FOIA/PA office is National Security Agency, ATTN: FOIA/PA Services (DC321), 9800 Savage Road, Suite 6248, Fort George G. Meade, MD 20755-6248. Individuals who have access to NSA/CSS spaces may send their request through the internal mail system to DC321.

(5) FOIA/PA Services (DC321) shall acknowledge the amendment request within 10 working days of receipt and respond within 30 working days. The organization/individual who originated the information under dispute shall be given 10 working days to comment. On receipt of a response, FOIA/PA Services (DC321) shall review all documentation and determine if the amendment request shall be granted. If FOIA/PA Services (DC321) agrees with the request, it shall notify the requester and the office holding the record. The latter shall promptly amend the record and notify all holders and recipients of the records of the correction. If the amendment request is denied, the requester shall be advised of the reasons for the denial and the procedures for filing an appeal.

(g) Appeal of Refusals To Amend Records—

(1) If the Director of Policy, as the Initial Denial Authority, refuses to amend any part of a record it shall notify the requester of its refusal, the reasons for the denial and the procedures for requesting a review of the decision by the NSA/CSS Appeal Authority. The Appeal Authority shall render a final decision within 30 working days, except when circumstances necessitate an extension. If an extension is necessary, the requester shall be informed, in writing, of the reasons for the delay and of the approximate date on which the review is expected to be completed. If the NSA/CSS Appeal Authority determines that the record should be amended, the requester, FOIA/PA Services, and the office holding the record

will be advised. The latter shall promptly amend the record and notify all recipients.

(2) If the NSA/CSS Privacy Act Appeal Authority denies any part of the request for amendment, the requester shall be advised of the reasons for denial, his or her right to file a concise statement of reasons for disputing the information contained in the record, and his or her right to seek judicial review of the Agency's refusal to amend the record. Statements of disagreement and related notifications and summaries of the Agency's reasons for refusing to amend the record shall be processed in the manner prescribed by 32 CFR part 310.

(h) Disclosures and Accounting of Disclosures.

(1) No record contained in a System of Records maintained within the Department of Defense shall be disclosed by any means of communication to any person, or to any agency outside the Department of Defense, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record will be:

(i) To those officials and employees of the Agency who have a need for the record in the performance of their duties and the use is compatible with the purpose for which the record is maintained.

(ii) Required to be disclosed under the Freedom of Information Act, as amended.

(iii) For a routine use as described in NSA/CSS systems of records notices. The DoD "Blanket Routine Uses" may also apply to NSA/CSS systems of records. (See Appendix C to 32 CFR part 310).

(iv) To the Bureau of the Census for the purpose of planning or carrying out a census or survey or related activity authorized by law.

(v) To a recipient who has provided the Department of Defense or the Agency with advance, adequate written assurance that:

(A) The record will be used solely as a statistical research or reporting record;

(B) The record is to be transferred in a form that is not individually identifiable (*i.e.*, the identity of the individual

cannot be determined by combining various statistical records); and

(C) The record will not be used to make any decisions about the rights, benefits, or entitlements of an individual.

(vi) To the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value. A record transferred to a Federal records center for safekeeping or storage does not fall within this category since Federal records center personnel act on behalf of the Department of Defense in this instance and the records remain under the control of the NSA/CSS. No disclosure accounting record of the transfer of records to Federal records center need be maintained.

(vii) To another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the NSA/CSS specifying the particular portion and the law enforcement activity for which the record is sought. Blanket requests for all records pertaining to an individual will not be accepted. A record may also be disclosed to a law enforcement agency at the initiative of the NSA/CSS when criminal conduct is suspected, provided that such disclosure has been established in advance as a "routine use."

(viii) To a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of the individual to whom the record pertains.

(ix) To Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, or any joint committee of Congress or subcommittee of any such joint committee. This does not authorize the disclosure of any record subject to this part to members of Congress acting in

their individual capacities or on behalf of their constituents, unless the individual consents.

(x) To the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office.

(xi) Pursuant to an order of a court of competent jurisdiction.

(A) When a record is disclosed under compulsory legal process and when the issuance of that order or subpoena is made public by the court that issued it, efforts shall be made to notify the individual to whom the record pertains. This may be accomplished by notifying the individual by mail at his most recent address as contained in the Component's records.

(B) Upon being served with an order to disclose a record, the General Counsel shall endeavor to determine whether the issuance of the order is a matter of public record and, if it is not, seek to be advised when it becomes public. An accounting of the disclosure shall be made at the time the NSA/CSS complies with the order or subpoena.

(xii) To a consumer reporting agency in accordance with section 3711(f) of Title 31.

(2) Except for disclosures made in accordance with paragraphs (h)(1)(i) and (ii) of this section, an accurate accounting of disclosures shall be kept by the record holder in consultation with the Privacy Act Coordinator.

(i) The accounting shall include the date, nature, and purpose of each disclosure of a record to any person or to another agency; and the name and address of the person or agency to whom the disclosure is made. There need not be a notation on a single document of every disclosure of a particular record, provided the record holder can construct from its System the required accounting information:

(A) When required by the individual;

(B) When necessary to inform previous recipients of any amended records, or

(C) When providing a cross reference to the justification or basis upon which the disclosure was made (including any written documentation as required in the case of the release of records for

statistical or law enforcement purposes).

(ii) The accounting shall be retained for at least five years after the last disclosure, or for the life of the record, whichever is longer. No record of the disclosure of this accounting need be maintained.

(iii) Except for disclosures made under paragraph (h)(1)(vii) of this section, the accounting of disclosures shall be made available to the individual to whom the record pertains. The individual shall submit a Privacy Act Information Request form to the Privacy Act Coordinator in the office keeping the accounting of disclosures.

(3) Disclosures made under circumstances not delineated in paragraphs (h)(1)(i) through (xii) of this section shall only be made after written permission of the individual involved has been obtained. Written permission shall be recorded on or appended to the document transmitting the personal information to the other agency, in which case no separate accounting of the disclosure need be made. Written permission is required in each separate case; *i.e.*, once obtained, written permission for one case does not constitute blanket permission for other disclosures.

(4) An individual's name and address may not be sold or rented unless such action is specifically authorized by law. This provision shall not be construed to require withholding of names and addresses otherwise permitted to be made public. Lists or compilations of names and home addresses, or single home addresses will not be disclosed, without the consent of the individual involved, to the public, including, but not limited to individual Congressmen, creditors, and commercial and financial institutions. Requests for home addresses may be referred to the last known address of the individual for reply at his discretion and the requester will be notified accordingly.

§ 322.6 Establishing exemptions.

(a) Neither general nor specific exemptions are established automatically for any system of records. The head of the DoD Component maintaining the system of records must make a determination whether the system is

one for which an exemption properly may be claimed and then propose and establish an exemption rule for the system. No system of records within the Department of Defense shall be considered exempt until the head of the Component has approved the exemption and an exemption rule has been published as a final rule in the FEDERAL REGISTER.

(b) No system of records within NSA/CSS shall be considered exempt under subsection (j) or (k) of the Privacy Act until the exemption rule for the system of records has been published as a final rule in the FEDERAL REGISTER.

(c) An individual is not entitled to have access to any information compiled in reasonable anticipation of a civil action or proceeding (5 U.S.C. 552a(d)(5)).

(d) Proposals to exempt a system of records will be forwarded to the Defense Privacy Office, consistent with the requirements of 32 CFR part 310, for review and action.

(e) Consistent with the legislative purpose of the Privacy Act of 1974, NSA/CSS will grant access to non-exempt material in the records being maintained. Disclosure will be governed by NSA/CSS's Privacy Regulation, but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal or civil violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered, the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of the above nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated above. The decisions to release information from these systems will be made on a case-by-case basis.

(f) Do not use an exemption to deny an individual access to any record to which he or she would have access under the Freedom of Information Act (5 U.S.C. 552).

(g) Disclosure of records pertaining to personnel, or the functions and activities of the National Security Agency shall be prohibited to the extent authorized by Pub. L. No. 86-36 (1959) and 10 U.S.C. 424.

(h) Exemptions NSA/CSS may claim.

(1) *General exemption.* The general exemption established by 5 U.S.C. 552a(j)(2) may be claimed to protect investigative records created and maintained by law enforcement activities of the NSA.

(2) *Specific exemptions.* The specific exemptions permit certain categories of records to be exempt from certain specific provisions of the Privacy Act.

(i) *(k)(1) exemption.* Information properly classified under Executive Order 12958 and that is required by Executive Order to be kept secret in the interest of national defense or foreign policy.

(ii) *(k)(2) exemption.* Investigatory information compiled for law-enforcement purposes by non-law enforcement activities and which is not within the scope of Sec. 310.51(a). If an individual is denied any right, privilege or benefit that he or she is otherwise entitled by federal law or for which he or she would otherwise be eligible as a result of the maintenance of the information, the individual will be provided access to the information except to the extent that disclosure would reveal the identity of a confidential source. This subsection when claimed allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(iii) *(k)(3) exemption.* Records maintained in connection with providing protective services to the President and other individuals identified under 18 U.S.C. 3506.

(iv) *(k)(4) exemption.* Records maintained solely for statistical research or program evaluation purposes and which are not used to make decisions on the rights, benefits, or entitlement of an individual except for census records which may be disclosed under 13 U.S.C. 8.

(v) *(k)(5) exemption.* Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified infor-

mation, but only to the extent such material would reveal the identity of a confidential source. This provision allows protection of confidential sources used in background investigations, employment inquiries, and similar inquiries that are for personnel screening to determine suitability, eligibility, or qualifications.

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

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

§ 322.7 Exempt systems of records.

(a) All systems of records maintained by the NSA/CSS and its components shall be exempt from the requirements of 5 U.S.C. 552a(d) pursuant to 5 U.S.C. 552a(k)(1) to the extent that the system contains any information properly classified under Executive Order 12958 and that is required by Executive Order to be kept secret in the interest of national defense or foreign policy. This exemption is applicable to parts of all systems of records including those not otherwise specifically designated for exemptions herein, which contain isolated items of properly classified information.

(b) GNSA 01.

(1) *System name:* Access, Authority and Release of Information File.

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

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

(3) **AUTHORITY:** 5 U.S.C. 552a(k)(5).

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

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

(c) GNSA 02.

(1) **System name:** Applicants.

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

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

(3) **AUTHORITY:** 5 U.S.C. 552a(k)(5).

(4) **Reasons:** (i) From subsection (c)(3) and (d) when access to accounting disclosures and access to or amendment of records would cause the identity of a confidential source to be revealed. Dis-

closure of the source's identity not only will result in the Department breaching the promise of confidentiality made to the source but it will impair the Department's future ability to compile investigatory material for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access to classified information. Unless sources can be assured that a promise of confidentiality will be honored, they will be less likely to provide information considered essential to the Department in making the required determinations.

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

(d) GNSA 03.

(1) **System name:** Correspondence, Cases, Complaints, Visitors, Requests.

(2) **Exemption:** (i) Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identity of a confidential source. **NOTE:** When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(ii) Records maintained solely for statistical research or program evaluation purposes and which are not used to make decisions on the rights, benefits, or entitlement of an individual except

for census records which may be disclosed under 13 U.S.C. 8, may be exempt pursuant to 5 U.S.C. 552a(k)(4).

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

(iv) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(2), (k)(4), and (k)(5) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) AUTHORITY: 5 U.S.C. 552a(k)(2), (k)(4), and (k)(5).

(4) *Reasons:* (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

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

(iii) From subsection (e)(1) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an in-

vestigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because there is no necessity for such publication since the system of records will be exempt from the underlying duties to provide notification about and access to information in the system and to make amendments to and corrections of the information in the system.

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NSA will, nevertheless, continue to publish such a notice in broad generic terms, as is its current practice.

(e) GNSA 04.

(1) *System name:* Military Reserve Personnel Data Base.

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

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

(3) AUTHORITY: 5 U.S.C. 552a(k)(5).

(4) *Reasons:* (i) From subsection (c)(3) and (d) when access to accounting disclosures and access to or amendment of records would cause the identity of a confidential sources to be revealed. Disclosure of the source's identity not only will result in the Department breaching the promise of confidentiality made to the source but it will impair the Department's future ability to compile investigatory material for the purpose of determining suitability, eligibility, or qualifications for Federal

civilian employment, Federal contracts, or access to classified information. Unless sources can be assured that a promise of confidentiality will be honored, they will be less likely to provide information considered essential to the Department in making the required determinations.

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

(f) GNSA 05.

(1) *System name:* Equal Employment Opportunity Data.

(2) *Exemption:* (i) Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identity of a confidential source. NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(ii) Records maintained solely for statistical research or program evaluation purposes and which are not used to make decisions on the rights, benefits, or entitlement of an individual except for census records which may be disclosed under 13 U.S.C. 8, may be exempt pursuant to 5 U.S.C. 552a(k)(4).

(iii) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(2) and (k)(4) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) AUTHORITY: 5 U.S.C. 552a(k)(2) and (k)(4).

(4) *Reasons:* (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

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

(iii) From subsection (e)(1) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because there is no necessity for such publication since the system of records will be exempt from the underlying duties to provide notification about and access to information in the system and to make amendments to and corrections of the information in the system.

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system

notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NSA will, nevertheless, continue to publish such a notice in broad generic terms, as is its current practice.

(g) GNSA 06.

(1) *System name:* Health, Medical and Safety Files.

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

(ii) Testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service may be exempt pursuant to 5 U.S.C. 552a(k)(6), if the disclosure would compromise the objectivity or fairness of the test or examination process.

(iii) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(5) and (k)(6) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) *AUTHORITY:* 5 U.S.C. 552a(k)(5) and (k)(6).

(4) *Reasons:* (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(ii) From subsections (d) and (f) because providing access to records of a civil or administrative investigation and the right to contest the contents of those records and force changes to be made to the information contained therein would seriously interfere with and thwart the orderly and unbiased conduct of the investigation and impede case preparation. Providing access rights normally afforded under the Privacy Act would provide the subject with valuable information that would

allow interference with or compromise of witnesses or render witnesses reluctant to cooperate; lead to suppression, alteration, or destruction of evidence; enable individuals to conceal their wrongdoing or mislead the course of the investigation; and result in the secreting of or other disposition of assets that would make them difficult or impossible to reach in order to satisfy any Government claim growing out of the investigation or proceeding.

(iii) From subsection (e)(1) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because there is no necessity for such publication since the system of records will be exempt from the underlying duties to provide notification about and access to information in the system and to make amendments to and corrections of the information in the system.

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NSA will, nevertheless, continue to publish such a notice in broad generic terms, as is its current practice.

(h) GNSA 08.

(1) *System name:* Payroll and Claims.

(2) *Exemption:* (i) Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identity of a confidential source. NOTE:

When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(ii) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(2) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) **AUTHORITY:** 5 U.S.C. 552a(k)(2).

(4) **Reasons:** (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

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

(iii) From subsection (e)(1) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because there is no necessity for such publication since the system of records will be exempt from the underlying duties to provide notification

about and access to information in the system and to make amendments to and corrections of the information in the system.

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NSA will, nevertheless, continue to publish such a notice in broad generic terms, as is its current practice.

(i) GNSA 09.

(1) **System name:** Personnel File.

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

(ii) Testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service may be exempt pursuant to 5 U.S.C. 552a(k)(6), if the disclosure would compromise the objectivity or fairness of the test or examination process.

(iii) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(5) and (k)(6) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) **AUTHORITY:** 5 U.S.C. 552a(k)(5) and (k)(6).

(4) **Reasons:** (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(ii) From subsections (d) and (f) because providing access to records of a civil or administrative investigation and the right to contest the contents of those records and force changes to be

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

(iii) From subsection (e)(1) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because there is no necessity for such publication since the system of records will be exempt from the underlying duties to provide notification about and access to information in the system and to make amendments to and corrections of the information in the system.

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NSA will, nevertheless, continue to publish such a notice in broad generic terms, as is its current practice.

(j) GNSA 10.

(1) *System name:* Personnel Security File.

(2) *Exemption:* (i) Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is

denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identity of a confidential source. NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

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

(iii) Testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service may be exempt pursuant to 5 U.S.C. 552a(k)(6), if the disclosure would compromise the objectivity or fairness of the test or examination process.

(iv) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(2), (k)(5), and (k)(6) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) *AUTHORITY:* 5 U.S.C. 552a(k)(2), (k)(5), and (k)(6).

(4) *Reasons:* (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(ii) From subsections (d) and (f) because providing access to records of a civil or administrative investigation and the right to contest the contents of those records and force changes to be made to the information contained therein would seriously interfere with and thwart the orderly and unbiased conduct of the investigation and impede case preparation. Providing access

rights normally afforded under the Privacy Act would provide the subject with valuable information that would allow interference with or compromise of witnesses or render witnesses reluctant to cooperate; lead to suppression, alteration, or destruction of evidence; enable individuals to conceal their wrongdoing or mislead the course of the investigation; and result in the secreting of or other disposition of assets that would make them difficult or impossible to reach in order to satisfy any Government claim growing out of the investigation or proceeding.

(iii) From subsection (e)(1) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because there is no necessity for such publication since the system of records will be exempt from the underlying duties to provide notification about and access to information in the system and to make amendments to and corrections of the information in the system.

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NSA will, nevertheless, continue to publish such a notice in broad generic terms, as is its current practice.

(k) GNSA 12.

(1) *System name*: Training.

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

(ii) Testing or examination material used solely to determine individual

qualifications for appointment or promotion in the Federal service may be exempt pursuant to 5 U.S.C. 552a(k)(6), if the disclosure would compromise the objectivity or fairness of the test or examination process.

(iii) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(5) and (k)(6) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) *AUTHORITY*: 5 U.S.C. 552a(k)(5), and (k)(6).

(4) *Reasons*: (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

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

(iii) From subsection (e)(1) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because there is no necessity for such publication since the system of

records will be exempt from the underlying duties to provide notification about and access to information in the system and to make amendments to and corrections of the information in the system.

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NSA will, nevertheless, continue to publish such a notice in broad generic terms, as is its current practice.

(l) GNSA 13.

(1) *System name:* Archival Records.

(2) *Exemption:* (i) Records maintained solely for statistical research or program evaluation purposes and which are not used to make decisions on the rights, benefits, or entitlement of an individual except for census records which may be disclosed under 13 U.S.C. 8, may be exempt pursuant to 5 U.S.C. 552a(k)(4).

(ii) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(4) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) *AUTHORITY:* 5 U.S.C. 552a(k)(4).

(4) *Reasons:* (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(ii) From subsections (d) and (f) because providing access to records of a civil or administrative investigation and the right to contest the contents of those records and force changes to be made to the information contained therein would seriously interfere with and thwart the orderly and unbiased conduct of the investigation and impede case preparation. Providing access rights normally afforded under the Privacy Act would provide the subject with valuable information that would

allow interference with or compromise of witnesses or render witnesses reluctant to cooperate; lead to suppression, alteration, or destruction of evidence; enable individuals to conceal their wrongdoing or mislead the course of the investigation; and result in the secreting of or other disposition of assets that would make them difficult or impossible to reach in order to satisfy any Government claim growing out of the investigation or proceeding.

(iii) From subsection (e)(1) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because there is no necessity for such publication since the system of records will be exempt from the underlying duties to provide notification about and access to information in the system and to make amendments to and corrections of the information in the system.

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NSA will, nevertheless, continue to publish such a notice in broad generic terms, as is its current practice.

(m) GNSA 14.

(1) *System name:* Library Patron File Control System.

(2) *Exemption:* (i) Records maintained solely for statistical research or program evaluation purposes and which are not used to make decisions on the rights, benefits, or entitlement of an individual except for census records which may be disclosed under 13 U.S.C. 8, may be exempt pursuant to 5 U.S.C. 552a(k)(4).

(ii) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(4) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d),

§ 322.7

32 CFR Ch. I (7-1-03 Edition)

(e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) *AUTHORITY:* 5 U.S.C. 552a(k)(4).

(4) *Reasons:* (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

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

(iii) From subsection (e)(1) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because there is no necessity for such publication since the system of records will be exempt from the underlying duties to provide notification about and access to information in the system and to make amendments to and corrections of the information in the system.

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system

notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NSA will, nevertheless, continue to publish such a notice in broad generic terms, as is its current practice.

(n) GNSA 15.

(1) *System name:* Computer Users Control System.

(2) *Exemption:* (i) Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identity of a confidential source. NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(ii) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(2) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) *AUTHORITY:* 5 U.S.C. 552a(k)(2).

(4) *Reasons:* (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(ii) From subsections (d) and (f) because providing access to records of a civil or administrative investigation and the right to contest the contents of those records and force changes to be made to the information contained therein would seriously interfere with and thwart the orderly and unbiased conduct of the investigation and impede case preparation. Providing access rights normally afforded under the Privacy Act would provide the subject

with valuable information that would allow interference with or compromise of witnesses or render witnesses reluctant to cooperate; lead to suppression, alteration, or destruction of evidence; enable individuals to conceal their wrongdoing or mislead the course of the investigation; and result in the secreting of or other disposition of assets that would make them difficult or impossible to reach in order to satisfy any Government claim growing out of the investigation or proceeding.

(iii) From subsection (e)(1) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because there is no necessity for such publication since the system of records will be exempt from the underlying duties to provide notification about and access to information in the system and to make amendments to and corrections of the information in the system.

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NSA will, nevertheless, continue to publish such a notice in broad generic terms, as is its current practice.

(o) GNSA 17.

(1) *System name:* Employee Assistance Service (EAS) Case Record System.

(2) *Exemption:* (i) Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the ex-

tent that disclosure would reveal the identity of a confidential source. NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(ii) Records maintained solely for statistical research or program evaluation purposes and which are not used to make decisions on the rights, benefits, or entitlement of an individual except for census records which may be disclosed under 13 U.S.C. 8, may be exempt pursuant to 5 U.S.C. 552a(k)(4).

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

(iv) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(2), (k)(4), and (k)(5) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) *AUTHORITY:* 5 U.S.C. 552a(k)(2), (k)(4), and (k)(5).

(4) *Reasons:* (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(ii) From subsections (d) and (f) because providing access to records of a civil or administrative investigation and the right to contest the contents of those records and force changes to be made to the information contained therein would seriously interfere with and thwart the orderly and unbiased conduct of the investigation and impede case preparation. Providing access rights normally afforded under the Privacy Act would provide the subject with valuable information that would allow interference with or compromise of witnesses or render witnesses reluctant to cooperate; lead to suppression, alteration, or destruction of evidence;

enable individuals to conceal their wrongdoing or mislead the course of the investigation; and result in the secreting of or other disposition of assets that would make them difficult or impossible to reach in order to satisfy any Government claim growing out of the investigation or proceeding.

(iii) From subsection (e)(1) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because there is no necessity for such publication since the system of records will be exempt from the underlying duties to provide notification about and access to information in the system and to make amendments to and corrections of the information in the system.

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NSA will, nevertheless, continue to publish such a notice in broad generic terms, as is its current practice.

(p) GNSA 18.

(1) *System name:* Operations Files.

(2) *Exemption:* (i) Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identity of a confidential source. NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a system of

records used in personnel or administrative actions.

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

(iii) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(2) and (k)(5) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f).

(3) AUTHORITY: 5 U.S.C. 552a(k)(2) and (k)(5).

(4) *Reasons:* (i) From subsection (c)(3) because the release of the disclosure accounting would place the subject of an investigation on notice that they are under investigation and provide them with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

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

(iii) From subsection (e)(1) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only

after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because there is no necessity for such publication since the system of records will be exempt from the underlying duties to provide notification about and access to information in the system and to make amendments and corrections to the information in the system.

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NSA will, nevertheless, continue to publish such a notice in broad generic terms, as is its current practice.

PART 323—DEFENSE LOGISTICS AGENCY PRIVACY PROGRAM

Sec.

323.1 Purpose and scope.

323.2 Policy.

323.3 Definitions.

323.4 Responsibilities.

323.5 Procedures.

323.6 Forms and reports.

APPENDIX A TO PART 323—INSTRUCTIONS FOR PREPARATION OF SYSTEM NOTICES

APPENDIX B TO PART 323—CRITERIA FOR NEW AND ALTERED RECORD SYSTEMS

APPENDIX C TO PART 323—INSTRUCTIONS FOR PREPARATION OF REPORTS TO NEW OR ALTERED SYSTEMS

APPENDIX D TO PART 323—WORD PROCESSING CENTER (WPC) SAFEGUARDS

APPENDIX E TO PART 323—OMB GUIDELINES FOR MATCHING PROGRAMS

APPENDIX F TO PART 323—LITIGATION STATUS SHEET

APPENDIX G TO PART 323—PRIVACY ACT ENFORCEMENT ACTIONS

APPENDIX H TO PART 323—DLA EXEMPTION RULES

AUTHORITY: Privacy Act of 1974, Pub. L. 93-579, Stat. 1896 (5 U.S.C. 552a).

SOURCE: DLAR 5400.21, 51 FR 33595, Sept. 22, 1986, unless otherwise noted. Redesignated at 56 FR 57803, Nov. 14, 1991.

§ 323.1 Purpose and scope.

This part 323 implements the Privacy Act of 1974 (5 U.S.C. 552a) and DoD Directive and DoD Regulation 5400.11, Department of Defense Privacy Program (32 CFR part 286a). It applies to Headquarters, Defense Logistics Agency (HQ DLA) and all DLA field activities.

§ 323.2 Policy.

It is the policy of DLA to safeguard personal information contained in any system of records maintained by DLA activities and to make that information available to the individual to whom it pertains to the maximum extent practicable. DLA policy specifically requires that DLA activities:

(a) Collect, maintain, use, and disseminate personal information only when it is relevant and necessary to achieve a purpose required by statute or Executive Order.

(b) Collect personal information directly from the individuals to whom it pertains to the greatest extent practical.

(c) Inform individuals who are asked to supply personal information for inclusion in any system of records:

(1) The authority for the solicitation.

(2) Whether furnishing the information is mandatory or voluntary.

(3) The intended uses of the information.

(4) The routine disclosures of the information that may be made outside DoD.

(5) The effect on the individual of not providing all of any part of the requested information.

(d) Ensure that all records used in making determinations about individuals are accurate, relevant, timely, and complete.

(e) Make reasonable efforts to ensure that records containing personal information are accurate, relevant, timely, and complete for the purposes for which they are being maintained before making them available to any recipients outside DoD, other than a Federal agency, unless the disclosure is made under DLAR 5400.14, DLA Freedom of Information Act Program (32 CFR part 1285).

(f) Keep no record that describes how individuals exercise their rights guaranteed by the First Amendment of the