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

(iv) From subsections (e)(4)(G) and (H) because this system of records is compiled for investigative purposes and is exempt from the access provisions of subsections (d) and (f).

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

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

[66 FR 52681, Oct. 17, 2001, as amended at 67 FR 55724, Aug. 30, 2002]

PART 321—DEFENSE SECURITY SERVICE PRIVACY PROGRAM

Sec.

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

SOURCE: 64 FR 49660, Sept. 14, 1999, unless otherwise noted.

§ 321.1 Purpose and applicability.

(a) This part establishes rules, policies and procedures for the disclosure of personal records in the custody of the Defense Security Service (DSS) to the individual subjects, the handling of requests for amendment or correction of such records, appeal and review of DSS decisions on these matters, and the application of general and specific exemptions, under the provisions of the Privacy Act of 1974. It also prescribes other policies and procedures to effect compliance with the Privacy Act of 1974 and DoD Directive 5400.11[1].

(b) The procedures set forth in this part do not apply to DSS personnel seeking access to records pertaining to themselves which previously have been available. DSS personnel will continue to be granted ready access to their personnel, security, and other records by making arrangements directly with the maintaining office. DSS personnel should contact the Office of Freedom of Information and Privacy, DSSHQ, for access to investigatory records pertaining to themselves or any assistance in obtaining access to other records pertaining to themselves, and may follow the procedures outlined in these rules in any case.

[1] Copies may be obtained via internet at http://web7.whs.osd.mil/corres.htm

§ 321.2 Definitions.

(a) All terms used in this part which are defined in 5 U.S.C. 552a shall have the same meaning herein.

(b) As used in this part, the term agency means the Defense Security Service.

§ 321.3 Information and procedures for requesting notification.

(a) *General.* Any individual may request and receive notification of whether he is the subject of a record in any system of records maintained by DSS using the information and procedures described in this section.

(1) Paragraphs (b) and (c) of this section give information that will assist an individual in determining in what systems of DSS records (if any) he may be the subject. This information is presented as a convenience to the individual in that he may avoid consulting the lengthy systems notices elsewhere in the Federal Register.

(2) Paragraph (d) of this section details the procedure an individual should use to contact DSS and request notification. It will be helpful if the individual states what his connection with DSS has or may have been, and about what record system(s) he is inquiring. Such information is not required, but its absence may cause some delay.

(b) *DSS Records Systems.* A list of DSS records systems is available by contacting Defense Security Service, Office of FOI and Privacy, 1340 Braddock Place, Alexandria, VA, 22314-1551.

(c) *Categories of individuals in DSS Record Systems.* (1) Any person who is the subject or co-subject of an ongoing or completed investigation by DSS should have an investigative case file/record in system V5-01, if the record meets retention criteria. An index to such files should be in V5-02.

(2) If an individual has ever made a formal request to DSS under the Freedom of Information Act or the Privacy Act of 1974, a record pertaining to that request under the name of the requester, or subject matter, will be in system V1-01.

(3) Persons of Counterintelligence interest who have solicited from industrial contractors/DoD installations information which may appear to be sensitive in nature may have a record in system V5-04.

(4) Individuals who have been applicants for employment with DSS, or nominees for assignment to DSS, but who have not completed their DSS affiliation, may be subjects in systems V4-04, V5-01, V5-02, V5-03, or V6-01.

(5) Any individual who is a subject, victim or cross-referenced personally in an investigation by an investigative element of any DoD component, may be referenced in the Defense Clearance and Investigations Index, system V5-02, in an index to the location, file number, and custodian of the case record.

(6) Individuals who have ever presented a complaint to or have been connected with a DSS Inspector General inquiry may be subjects of records in system V2-01.

(7) If an individual has ever attended the Defense Industrial Security Institute or completed training with the DSS Training Office he should be subject of a record in V7-01.

(8) If an individual has ever been a guest speaker or instructor at the Defense Industrial Security Institute, he should be the subject of a record in V7-01.

(9) If an individual is an employee or major stockholder of a government contractor or other DoD-affiliated company or agency and has been issued, now possesses or has been processed for a security clearance, he may be subject to a record in V5-03.

(d) *Procedures.* The following procedures should be followed to determine if an individual is a subject of records maintained by DSS, and to request notification and access.

(1) Individuals should submit inquiries in person or by mail to the Defense Security Service, Office of FOI and Privacy, 1340 Braddock Place, Alexandria, VA 22314-1651. Inquiries by personal appearance should be made Monday through Friday from 8:30 to 11:30 a.m. and 1:00 to 4:00 p.m. The information requested in Sec. 321.4 must be provided if records are to be accurately identified. Telephonic requests for records will not be honored. In a case where the system of records is not specified in the request, only systems that would reasonably contain records

of the individual will be checked, as described in paragraph (b) of this section.

(2) Only the Director or Chief, Office of FOI and Privacy may authorize exemptions to notification of individuals in accordance with § 321.13.

§ 321.4 Requirements for identification.

(a) *General.* Only upon proper identification, made in accordance with the provisions of this section, will any individual be granted notification concerning and access to all releasable records pertaining to him which are maintained in a DSS system.

(b) *Identification.* Identification of individuals is required both for accurate record identification and to verify identity in order to avoid disclosing records to unauthorized persons. Individuals who request notification of, access to, or amendment of records pertaining to themselves, must provide their full name (and additional names such as aliases, maiden names, alternate spellings, etc., if a check of these variants is desired), date and place of birth, and social security number (SSN).

(1) Where reply by mail is requested, a mailing address is required, and a telephone number is recommended to expedite certain matters. For military requesters residing in the United States, home address or P.O. Box number is preferred in lieu of duty assignment address.

(2) Signatures must be notarized on requests received by mail. Exceptions may be made when the requester is well known to releasing officials. For requests made in person, a photo identification card, such as military ID, driver's license or building pass, must be presented.

(3) While it is not required as a condition of receiving notification, in many cases the SSN may be necessary to obtain an accurate search of DCII (V5-02) records.

(c) A DSS Form 30 (Request for Notification of/Access to Personal Records) will be provided to any individual inquiring about records pertaining to himself whose mailed request was not notarized. This form is also available at the DSS Office of FOI and Privacy, 1340 Braddock Place, Alexandria, VA 22314-1651, for those who make their requests in person.

§ 321.5 Access by subject individuals.

(a) *General.* (1) Individuals may request access to records pertaining to themselves in person or by mail in accordance with this section. However, nothing in this section shall allow an individual access to any information compiled or maintained by DSS in reasonable anticipation of a civil or criminal action or proceeding, or otherwise exempted under the provisions of § 321.13.

(2) A request for a pending personnel security investigation will be held in abeyance until completion of the investigation and the requester will be so notified.

(b) *Manner of access.* (1) Requests by mail or in person for access to DSS records should be made to the DSS Office of FOI and Privacy, 1340 Braddock Place, Alexandria, VA 22314-1651.

(2) Any individual who makes a request for access in person shall:

(i) Provide identification as specified in Sec. 321.4.

(ii) Complete and sign a request form.

(3) Any individual making a request for access to records by mail shall include a signed and notarized statement to verify his identity, which may be the DSS request form if he has received one.

(4) Any individual requesting access to records in person may be accompanied by an identified person of his own choosing while reviewing the record. If the individual elects to be accompanied, he shall make this known in his written request, and include a statement authorizing disclosure of the record contents to the accompanying person. Without written authorization of the subject individual, records will not be disclosed to third parties accompanying the subject.

(5) During the course of official business, members of DSS field elements may be given access to records maintained by the field elements/Operations Center without referral to the Office of FOI and Privacy. An account of such access will be kept for reporting purposes.

(6) In all requests for access, the requester must state whether he or she

desires access in person or mailed copies of records. During personal access, where copies are made for retention, a fee for reproduction and postage may be assessed as provided in Sec. 321.11. Where copies are mailed because personal appearance is impractical, there will be no fee.

(7) All individuals who are not affiliates of DSS will be given access to records, if authorized, in the Office of FOI and Privacy, or by means of mailed copies.

§ 321.6 Medical records.

General. Medical records that are part of DSS records systems will generally be included with those records when access is granted to the subject to which they pertain. However, if it is determined that such access could have an adverse effect upon the individual's physical or mental health, the medical record in question will be released only to a physician named by the requesting individual.

§ 321.7 Request for correction or amendment.

(a) *General.* Upon request and proper identification by any individual who has been granted access to DSS records pertaining to himself or herself, that individual may request, either in person or through the mail, that the record be amended. Such a request must be made in writing and addressed to the Defense Security Service, Office of FOI and Privacy, 1340 Braddock Place, Alexandria, VA 22314-1651.

(b) *Content.* The following information must be included to insure effective action on the request:

(1) Description of the record. Requesters should specify the number of pages and documents, the titles of the documents, form numbers if there are any, dates on the documents and names of individuals who signed them. Any reasonable description of the document is acceptable.

(2) Description of the items to be amended. The description of the passages, pages or documents to be amended should be as clear and specific as possible.

(i) Page, line and paragraph numbers should be cited where they exist.

(ii) A direct quotation of all or a portion of the passage may be made if it isn't otherwise easily identifiable. If the passage is long, a quotation of its beginning and end will suffice.

(iii) In appropriate cases, a simple substantive request may be appropriate, e.g., 'delete all references to my alleged arrest in July 1970.'

(iv) If the requester has received a copy of the record, he may submit an annotated copy of documents he wishes amended.

(3) Type of amendment. The requester must clearly state the type of amendment he is requesting.

(i) Deletion or expungement, i.e., a complete removal from the record of data, sentences, passages, paragraphs or documents.

(ii) Correction of the information in the record to make it more accurate, e.g., rectify mistaken identities, dates, data pertaining to the individual, etc.

(iii) Additions to make the record more relevant, accurate or timely may be requested.

(iv) Other changes may be requested; they must be specifically and clearly described.

(4) Reason for amendment. Requests for amendment must be based on specific reasons, included in writing. Categories of reasons are as follows:

(i) Accuracy. Amendment may be requested where matters of fact are believed incorrectly recorded, e.g., dates, names, addresses, identification numbers, or any other information concerning the individual. The request, whenever possible, should contain the accurate information, copies of verifying documents, or indication of how the information can be verified.

(ii) Relevance. Amendment may be requested when information in a record is believed not to be relevant or necessary to the purposes of the record system.

(iii) Timeliness. Amendment may be requested when information is thought to be so old as to no longer be pertinent to the stated purposes of the records system. It may also be requested when there is recent information of a pertinent type that is not included in the record.

(iv) Completeness. Amendment may be requested where information in a

record is incomplete with respect to its purpose. The data thought to have been omitted should be included or identified with the request.

(v) Fairness. Amendment may be requested when a record is thought to be unfair concerning the subject, in terms of the stated purposes of the record. In such cases, a source of additional information to increase the fairness of the record should be identified where possible.

(vi) Other reasons. Reasons for requesting amendment are not limited to those cited above. The content of the records is authorized in terms of their stated purposes which should be the basis for evaluating them. However, any matter believed appropriate may be submitted as a basis of an amendment request.

(vii) Court orders and statutes may require amendment of a file. While they do not require a Privacy Act request for execution, such may be brought to the attention of DSS by these procedures.

(c) *Assistance.* Individuals seeking to request amendment of records pertaining to themselves that are maintained by DSS will be assisted as necessary by DSS officials. Where a request is incomplete, it will not be denied, but the requester will be contacted for the additional information necessary to his request.

(d) This section does not permit the alteration of evidence presented to courts, boards and other official proceedings.

§ 321.8 DSS review of request for amendment.

(a) *General.* Upon receipt from any individual of a request to amend a record pertaining to himself and maintained by the Defense Security Service, Office of FOI and Privacy will handle the request as follows:

(1) A written acknowledgment of the receipt of a request for amendment of a record will be provided to the individual within 10 working days, unless final action regarding approval or denial can be accomplished within that time. In that case, the notification of approval or denial will constitute adequate acknowledgment.

(2) Where there is a determination to grant all or a portion of a request to amend a record, the record shall be promptly amended and the requesting individual notified. Individuals, agencies or components shown by accounting records to have received copies of the record, or to whom disclosure has been made, will be notified, if necessary, of the amendment by the responsible official. Where a DoD recipient of an investigative record cannot be located, the notification, if necessary, will be sent to the personnel security element of the parent Component.

(3) Where there is a determination to deny all or a portion of a request to amend a record, the office will promptly:

(i) Advise the requesting individual of the specifics of the refusal and the reasons;

(ii) Inform the individual that he may request a review of the denial(s) from 'Director, Defense Security Service, 1340 Braddock Place, Alexandria, VA 22314-1651.' The request should be brief, in writing, and enclose a copy of the denial correspondence.

(b) DSS determination to approve or deny. Determination to approve or deny and request to amend a record or portion thereof may necessitate additional investigation or inquiry be made to verify assertions of individuals requesting amendment. Coordination will be made with the Director for Investigations and the Director of the Personnel Investigations Center in such instances.

§ 321.9 Appeal of initial amendment decision.

(a) *General.* Upon receipt from any individual of an appeal to review a DSS refusal to amend a record, the Defense Security Service, Office of FOI and Privacy will assure that such appeal is handled in compliance with the Privacy Act of 1974 and DoD Directive 5400.11 and accomplish the following:

(1) Review the record, request for amendment, DSS action on the request and the denial, and direct such additional inquiry or investigation as is deemed necessary to make a fair and equitable determination.

(2) Recommend to the Director whether to approve or deny the appeal.

(3) If the determination is made to amend a record, advise the individual and previous recipients (or an appropriate office) where an accounting of disclosures has been made.

(4) Where the decision has been made to deny the individual's appeal to amend a record, notify the individual:

(i) Of the denial and the reason;

(ii) Of his right to file a concise statement of reasons for disagreeing with the decision not to amend the record;

(iii) That such statement may be sent to the Defense Security Service, Office of FOI and Privacy, (GCF), 1340 Braddock Place, Alexandria, VA 22314-1651, and that it will be disclosed to users of the disputed record;

(iv) That prior recipients of the disputed record will be provided a copy of the statement of disagreement, or if they cannot be reached (e.g., through deactivation) the personnel security element of their DoD component;

(v) And, that he may file a suit in a Federal District Court to contest DSS's decision not to amend the disputed record.

(b) *Time limit for review of appeal.* If the review of an appeal of a refusal to amend a record cannot be accomplished within 30 days, the Office of FOI and Privacy will notify the individual and advise him of the reasons, and inform him of when he may expect the review to be completed.

§ 321.10 Disclosure to other than subject.

(a) *General.* No record contained in a system of records maintained by DSS shall be disclosed by any means to any person or agency outside the Department of Defense, except with the written consent or request of the individual subject of the record, except as provided in this section. Disclosures that may be made without the request or consent of the subject of the record are as follows:

(1) To those officials and employees of the Department of Defense who have a need for the record in the performance of their duties, when the use is compatible with the stated purposes for which the record is maintained.

(2) Required to be disclosed by the Freedom of Information Act.

(3) For a routine use as described in DoD Directive 5400.11.

(4) To the Census Bureau, National Archives, the U.S. Congress, the Comptroller General or General Accounting Office under the conditions specified in DoD Directive 5400.11.

(5) At the written request of the head of an agency outside DoD for a law enforcement activity as authorized by DoD Directive 5400.11.

(6) For statistical purposes, in response to a court order, or for compelling circumstances affecting the health or safety of an individual as described in DoD Directive 5400.11.

(7) Legal guardians recognized by the Act.

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

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

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

(3) An accounting of disclosures made to agencies outside the DoD of records in the Defense Clearance and Investigations Index (V5-02) will be kept as prescribed by the Director of Systems, DSS.

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

(5) Subjects of DSS records will be given access to associated accounting records upon request, except as exempted under § 321.13.

§ 321.11 Fees.

Individuals may request copies for retention of any documents to which they are granted access in DSS records pertaining to them. Requestors will not be charged for the first copy of any records provided; however, duplicate

copies will require a charge to cover costs of reproduction. Such charges will be computed in accordance with DoD Directive 5400.11.

§ 321.12 Penalties.

(a) An individual may bring a civil action against the DSS to correct or amend the record, or where there is a refusal to comply with an individual request or failure to maintain any record with accuracy, relevance, timeliness and completeness, so as to guarantee fairness, or failure to comply with any other provision of 5 U.S.C. 552a. The court may order correction or amendment. It may assess against the United States reasonable attorney fees and other costs, or may enjoin the DSS from withholding the records and order the production to the complainant.

(b) Where it is determined that the action was willful or intentional with respect to 5 U.S.C. 552a(g)(1) (C) or (D), the United States shall be liable for the actual damages sustained, but in no case less than the sum of $1,000 and the costs of the action with attorney fees.

(c) Criminal penalties may be imposed against an officer or employee of the DSS who fully discloses material, which he knows is prohibited from disclosure, or who willfully maintains a system of records without the notice requirements; or against any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses. These offenses shall be misdemeanors with a fine not to exceed $5,000.

§ 321.13 Exemptions.

(a) *General.* The Director of the Defense Security Service establishes the following exemptions of records systems (or portions thereof) from the provisions of these rules, and other indicated portions of Pub. L. 93-579, in this section. They may be exercised only by the Director, Defense Security Service and the Chief of the Office of FOI and Privacy. Exemptions will be exercised only when necessary for a specific, significant and legitimate reason connected with the purpose of a records system, and not simply because they are authorized by statute. Personal records releasable under the provisions of 5 U.S.C. 552 will not be withheld from subject individuals based on these exemptions.

(b) All systems of records maintained by DSS shall be exempt from the requirements of 5 U.S.C. 552a(d) pursuant to 5 U.S.C. 552a(k)(1) to the extent that the system contains any information properly classified under Executive Order 12958 and which is required by the Executive Order to be withheld in the interest of national defense of foreign policy. This exemption, which may be applicable to parts of all systems of records, is necessary because certain record systems not otherwise specifically designated for exemptions herein may contain items of information that have been properly classified.

(c) *System identifier:* V1-01.

(1) System name: Privacy and Freedom of Information Request Records.

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

(ii) Records maintained in connection with providing protective services to the President and other individuals under 18 U.S.C. 3506, may be exempt pursuant to 5 U.S.C. 552a(k)(3).

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

(iv) Any portion of this system that falls under the provisions of 5 U.S.C. 552a(k)(2), (k)(3), (k)(5) may be exempt from the following subsections of 5 U.S.C. 552a(c)(3); (d); (e)(1); (e)(4)(G), (H) and (I); and (f).

(3) Authority: 5 U.S.C. 552a(k)(2), (k)(3), (k)(5).

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

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

(iii) From subsections (d) and (f) because requiring DSS to grant access to records and agency rules for access and amendment of records would unfairly impede the agency's investigation of allegations of unlawful activities. To require DSS to confirm or deny the existence of a record pertaining to a requesting individual may in itself provide an answer to that individual relating to an on-going investigation. The investigation of possible unlawful activities would be jeopardized by agency rules requiring verification of record, disclosure of the record to the subject, and record amendment procedures.

(d) *System identifier:* V5-01.

(1) System name: Investigative Files System

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

(ii) Records maintained in connection with providing protective services to the President and other individuals under 18 U.S.C. 3506, may be exempt pursuant to 5 U.S.C. 552a(k)(3).

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

(iv) Any portion of this system that falls under the provisions of 5 U.S.C. 552a(k)(2), (k)(3), or (k)(5) may be exempt from the following subsections of 5 U.S.C. 552a(c)(3); (d); (e)(1); (e)(4)(G), (H), and (I); and (f).

(3) Authority: 5 U.S.C. 552a(k)(2), (k)(3), or (k)(5).

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

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

(iii) From subsections (d) and (f) because requiring DSS to grant access to records and agency rules for access and amendment of records would unfairly impede the agency's investigation of allegations of unlawful activities. To require DSS to confirm or deny the existence of a record pertaining to a requesting individual may in itself provide an answer to that individual relating to an on-going investigation. The investigation of possible unlawful activities would be jeopardized by agency rules requiring verification of record, disclosure of the record to the subject, and record amendment procedures.

(e) *System identifier:* V5-02.

(1) System name: Defense Clearance and Investigations Index (DCII).

(2) Exemption: Investigatory material compiled for law enforcement purposes may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source. Any portion of this system that falls under the provisions of 5 U.S.C. 552a(k)(2) may be exempt from the following subsections of 5 U.S.C. 552a(c)(3); (d); (e)(1); (e)(4)(G), (H), and (I), and (f).

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

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

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

(iii) From subsections (d) and (f) because requiring DSS to grant access to records and agency rules for access and amendment of records would unfairly impede the agency's investigation of allegations of unlawful activities. To require DSS to confirm or deny the existence of a record pertaining to a requesting individual may in itself provide an answer to that individual relating to an on-going investigation. The investigation of possible unlawful activities would be jeopardized by agency rules requiring verification of record, disclosure of the record to the subject, and record amendment procedures.

(f) *System identifier:* V5-03.

(1) System name: Case Control Management System (CCMS).

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

(ii) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source. Any portion of this system that falls under the provisions of 5 U.S.C. 552a(k)(2) or (k)(5) may be exempt from the following subsections of 5 U.S.C. 552a: (c)(3); (d); (e)(1); (e)(4)(G), (H), and (I); and (f).

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

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

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

(iii) From subsections (d) and (f) because requiring DSS to grant access to records and agency rules for access and amendment of records would unfairly impede the agency's investigation of allegations of unlawful activities. To require DSS to confirm or deny the existence of a record pertaining to a requesting individual may in itself provide an answer to that individual relating to an on-going investigation. The investigation of possible unlawful activities would be jeopardized by agency rules requiring verification of record, disclosure of the record to the subject, and record amendment procedures.

(g) *System identifier:* V5-04.

(1) System name: Counterintelligence Issues Database (CII-DB).

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

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

(iii) Records maintained in connection with providing protective services to the President and other individuals under 18 U.S.C. 3506, may be exempt pursuant to 5 U.S.C. 552a(k)(3).

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

(v) Any portion of this system that falls within the provisions of 5 U.S.C. 552a(k)(1), (k)(2), (k)(3) and (k)(5) may be exempt from the following subsections (c)(3); (d)(1) through (d)(5); (e)(1); (e)(4)(G), (H), and (I); and (f).

(3) Authority. 5 U.S.C. 552a(k)(1), (k)(2), (k)(3) and (k)(5).

(4) Reasons. (i) From subsection (c)(3) because giving the individual access to the disclosure accounting could alert the subject of an investigation to the existence and nature of the investigation and reveal investigative or prosecutive interest by other agencies, particularly in a joint-investigation situation. This would seriously impede or compromise the investigation and case preparation by prematurely revealing its existence and nature; compromise or interfere with witnesses or make witnesses reluctant to cooperate with the investigators; lead to suppression, alteration, fabrication, or destruction of evidence; and endanger the physical safety of confidential sources, witnesses, law enforcement personnel and their families.

(ii) From subsection (d) because the application of these provisions could impede or compromise an investigation or prosecution if the subject of an investigation had access to the records or were able to use such rules to learn of the existence of an investigation before

it would be completed. In addition, the mere notice of the fact of an investigation could inform the subject and others that their activities are under or may become the subject of an investigation and could enable the subjects to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

(iii) From subsection (e)(1) because during an investigation it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear. In other cases, what may appear to be a relevant and necessary piece of information may become irrelevant in light of further investigation. In addition, during the course of an investigation, the investigator may obtain information that related primarily to matters under the investigative jurisdiction of another agency, and that information may not be reasonably segregated. In the interest of effective law enforcement, DSS investigators should retain this information, since it can aid in establishing patterns of criminal activity and can provide valuable leads for Federal and other law enforcement agencies.

(iv) From subsections (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f) because this system is exempt from subsection (d) of the Act, concerning access to records. These requirements are inapplicable to the extent that these records will be exempt from these subsections. However, DSS has published information concerning its notification and access procedures, and the records source categories because under certain circumstances, DSS could decide it is appropriate for an individual to have access to all or a portion of his/her records in this system of records.

§ 321.14 DSS implementation policies.

(a) *General.* The implementation of the Privacy Act of 1974 within DSS is as prescribed by DoD Directive 5400.11. This section provides special rules and information that extend or amplify DoD policies with respect to matters of particular concern to the Defense Security Service.

(b) *Privacy Act rules application.* Any request which cites neither Act, concerning personal record information in a system or records, by the individual to whom such information pertains, for access, amendment, correction, accounting of disclosures, etc., will be governed by the Privacy Act of 1974, DoD Directive 5400.11 and these rules exclusively. Requests for like information which cite only the Freedom of Information Act will be governed by the Freedom of Information Act, DoD Regulation 5400.7R [2]. Any denial or exemption of all or part of a record from notification, access, disclosure, amendment or other provision, will also be processed under these rules, unless court order or other competent authority directs otherwise.

(c) *First amendment rights.* No DSS official or element may maintain any information pertaining to the exercise by an individual of his rights under the First Amendment without the permission of that individual unless such collection is specifically authorized by statute or necessary to and within the scope of an authorized law enforcement activity.

(d) *Standards of accuracy and validation of records.* (1) All individuals or elements within DSS which create or maintain records pertaining to individuals will insure that they are reasonably accurate, relevant, timely and complete to serve the purpose for which they are maintained and to assure fairness to the individual to whom they pertain. Information that is not pertinent to a stated purpose of a system of records will not be maintained within those records. Officials compiling investigatory records will make every reasonable effort to assure that only reports that are impartial, clear, accurate, complete, fair and relevant with respect to the authorized purpose of such records are included, and that reports not meeting these standards or serving such purposes are not included in such records.

(2) Prior to dissemination to an individual or agency outside DoD of any record about an individual (except for a

[2] See footnote 1 to 321.1.

Freedom of Information Act action or access by a subject individual under these rules) the disclosing DSS official will by review, make a reasonable effort to assure that such record is accurate, complete, timely, fair and relevant to the purpose for which they are maintained.

(e) *The Defense Clearance and Investigations Index (DCII).* It is the policy of DSS, as custodian, that each DoD component or element that has direct access to or contributes records to the DCII (V5-02), is individually responsible for compliance with the Privacy Act of 1974 and DoD Directive 5400.11 with respect to requests for notification, requests for access by subject individuals, granting of such access, request for amendment and corrections by subjects, making amendments or corrections, other disclosures, accounting for disclosures and the exercise of exemptions, insofar as they pertain to any record placed in the DCII by that component or element. Any component or element of the DoD that makes a disclosure of any record whatsoever to an individual or agency outside the DoD, from the DCII, is individually responsible to maintain an accounting of that disclosure as prescribed by the Privacy Act of 1974 and DoD Directive 5400.11 and to notify the element placing the record in the DCII of the disclosure. Use of and compliance with the procedures of the DCII Disclosure Accounting System will meet these requirements. Any component or element of DoD with access to the DCII that, in response to a request concerning an individual, discovers a record pertaining to that individual placed in the DCII by another component or element, may refer the requester to the DoD component that placed the record into the DCII without making an accounting of such referral, although it involves the divulging of the existence of that record. Generally, consultation with, and referral to, the component or element placing a record in the DCII should be effected by any component receiving a request pertaining to that record to insure appropriate exercise of amendment or exemption procedures.

(f) *Investigative operations.* (1) DSS agents must be thoroughly familiar with and understand these rules and the authorities, purposes and routine uses of DSS investigative records, and be prepared to explain them and the effect of refusing information to all sources of investigative information, including subjects, during interview, in response to questions that go beyond the required printed and oral notices. Agents shall be guided by DSS Handbook for Personnel Security Investigations in this respect.

(2) All sources may be advised that the subject of an investigative record may be given access to it, but that the identities of sources may be withheld under certain conditions. Such advisement will be made as prescribed in DSS Handbook for Personnel Security Investigations, and the interviewing agent may not urge a source to request a grant of confidentiality. Such pledges of confidence will be given sparingly and then only when required to obtain information relevant and necessary to the stated purpose of the investigative information being collected.

(g) *Non-system information on individuals.* The following information is not considered part of personal records systems reportable under the Privacy Act of 1974 and may be maintained by DSS members for ready identification, contact, and property control purposes only. If at any time the information described in this paragraph is to be used for other than these purposes, that information must become part of a reported, authorized record system. No other information concerning individuals except that described in the records systems notice and this paragraph may be maintained within DSS.

(1) Identification information at doorways, building directories, desks, lockers, name tags, etc.

(2) Identification in telephone directories, locator cards and rosters.

(3) Geographical or agency contact cards.

(4) Property receipts and control logs for building passes, credentials, vehicles, weapons, etc.

(5) Temporary personal working notes kept solely by and at the initiative of individual members of DSS to facilitate their duties.

(h) *Notification of prior recipients.* Whenever a decision is made to amend a record, or a statement contesting a

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

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

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

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

Sec.

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