

Records Service, Office of Records Management. The GSA and NARA procedures and guidelines will be adapted and modified as required to meet DISA needs.

(2) Be responsible for providing the "Forms" which are required to comply with 32 CFR 310.9(b).

(f) The Assistant to the Director for Personnel, Headquarters, DISA will:

(1) Be responsible for development, within DISA, of an appropriate training program for all DISA personnel whose duties involve responsibilities for systems of records affected by the Privacy Act.

(2) Assure that DISA personnel involved in the design, development, operation, or maintenance of any system of records, as defined in 32 CFR 310.6 are informed of all requirements to protect the privacy of the individuals who are subjects of the records. The criminal penalties and civil suit aspects of the Privacy Act will be emphasized.

(3) Assure that within DISA administrative and physical safeguards are established to protect information from unauthorized or unintentional access, disclosure, modification or destruction and to insure that all persons whose official duties require access to or processing and maintenance of personal information are trained in the proper safeguarding and use of such information.

[40 FR 55535, Nov. 28, 1975. Redesignated and amended at 57 FR 6074, Feb. 20, 1992; 62 FR 26389, May 14, 1997]

§ 316.7 Questions.

Questions on both the substance and procedure of the Privacy Act and the DISA implementation thereof should be addressed to the DISA Counsel by the most expeditious means possible, including telephone calls.

[40 FR 55535, Nov. 28, 1975. Redesignated at 57 FR 6074, Feb. 20, 1992, as amended at 62 FR 26390, May 14, 1997]

§ 316.8 Exemptions.

Section 5 U.S.C. 552a (3)(j) and (3)(k) authorize an agency head to exempt certain systems of records or parts of certain systems of records from some of the requirements of the act. This part reserves to the Director, DISA, as

head of an agency, the right to create exemptions pursuant to the exemption provisions of the act. All systems of records maintained by DISA shall be exempt from the requirements of 5 U.S.C. 552a (d) pursuant to 5 U.S.C. 552a(3)(k)(l) to the extent that the system contains any information properly classified under Executive Order 11652, "Classification and Declassification of National Security Information and Material," dated March 8, 1972 (37 FR 10053, May 19, 1972) and which is required by the executive order to be kept secret in the interest of national defense or foreign policy. This exemption, which may be applicable to parts of all systems of records, is necessary because certain record systems not otherwise specifically designated for exemptions may contain isolated information which has been properly classified.

[42 FR 20298, Apr. 19, 1977. Redesignated at 57 FR 6074, Feb. 20, 1992, as amended at 62 FR 26390, May 14, 1997]

PART 317—DEFENSE CONTRACT AUDIT AGENCY PRIVACY ACT PROGRAM

Subpart A—General Provisions

Sec.

- 317.1 Purpose.
- 317.2 Applicability and scope.
- 317.3 Definitions.
- 317.4 Policy.
- 317.5 Responsibilities.
- 317.6 Procedures.

Subpart B—Systems of Records

- 317.10 General.
- 317.11 Federal Government contractors.
- 317.12 Safeguarding information in systems of records.

Subpart C—Collecting Information About Individuals

- 317.20 General considerations.
- 317.21 Forms.

Subpart D—Access to Records

- 317.30 Individual access to records.
- 317.31 Reproduction fees.
- 317.32 Denying individual access.
- 317.33 Privacy Act case files.

§ 317.1

Subpart E—Amendment of Records

- 317.40 Individual review and amendment.
- 317.41 Amending records.
- 317.42 Burden of proof.
- 317.43 Verifying identity.
- 317.44 Limits on amending judicial and quasi-judicial evidence and findings.
- 317.45 Standards for amendment request determinations.
- 317.46 Time limits.
- 317.47 Granting an amendment request in whole or in part.
- 317.48 Denying an amendment request in whole or in part.
- 317.49 Appeal procedures.
- 317.50 Requests for amending OPM records.
- 317.51 Individual's statement of disagreement.
- 317.52 Agency's statement of reasons.

Subpart F—Disclosure of Records

- 317.60 Conditions of disclosure.
- 317.61 Non-consensual disclosures.
- 317.62 Disclosures to commercial enterprises.
- 317.63 Disclosing health care records to the public.
- 317.64 Accounting for disclosures.

Subpart G—Publication Requirements

- 317.70 Federal Register publication.
- 317.71 Exemption rules.
- 317.72 System of records notices.
- 317.73 New and altered record systems.
- 317.74 Amendment and deletion of system notices.

Subpart H—Training Requirements

- 317.80 Statutory training requirements.
- 317.81 DCAA training programs.

Subpart I—Computer Matching Program Procedures

- 317.90 General.
- 317.91 Federal personnel or payroll record matches.
- 317.92 Federal benefit matches.
- 317.93 Matching program exclusions.
- 317.94 Conducting matching programs.
- 317.95 Providing due process to matching subjects.
- 317.96 Matching program agreement.
- 317.97 Cost-benefit analysis.
- 317.98 Appeals of denials of matching agreements.
- 317.99 Proposals for matching programs.

Subpart J—Enforcement Actions

- 317.110 Administrative remedies.
- 317.111 Civil court actions.
- 317.112 Criminal penalties.
- 317.113 Litigation status report.

32 CFR Ch. I (7–1–99 Edition)

- 317.114 Annual review of enforcement actions.

Subpart K—Reports

- 317.120 Report requirements.
- 317.121 Reports.

Subpart L—Agency Exemption Rules

- 317.130 Establishing and using exemptions.
 - 317.131 General exemptions.
 - 317.132 Specific exemptions.
 - 317.133 DCAA exempt record systems.
- APPENDIX A TO PART 317—DCAA BLANKET ROUTINE USES
- APPENDIX B TO PART 317—PROVISIONS OF THE PRIVACY ACT FROM WHICH A GENERAL OR SPECIFIC EXEMPTION MAY BE CLAIMED
- APPENDIX C TO PART 317—LITIGATION STATUS REPORT

AUTHORITY: Privacy Act of 1974, Pub. L. 93-579, 88 Stat. 1896 (5 U.S.C. 552a).

SOURCE: 57 FR 48992, Oct. 29, 1992, unless otherwise noted.

Subpart A—General Provisions

§ 317.1 Purpose.

(a) This part consolidates into a single document, the Defense Contract Audit Agency policies and procedures for implementing the Privacy Act of 1974 (5 U.S.C. 552a), as amended, by authorizing the development, publication and maintenance of the DCAA Privacy Act Program set forth by DCAA Regulation 5410.10¹, "Privacy Act Program", and DCAA Manual 5410.16², "DCAA Privacy Act Processing Guide."

(b) Its purpose is to delegate authorities and assign responsibilities for the administration of the DCAA Privacy Act Program and to prescribe uniform procedures for agency personnel consistent with DoD 5025.1-M³, "DoD Directives System Procedures."

§ 317.2 Applicability and scope.

(a) This part applies to all DCAA organizational elements and takes precedence over all regional regulatory

¹Copies may be obtained, at cost, from the Defense Contract Audit Agency, ATTN: CMO, Cameron Station, Alexandria, VA 22304-6178.

²See footnote 1 to § 317.1(a).

³Copies may be obtained, at cost, from the National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.

issuances that supplement the DCAA Privacy Program.

(b) This part shall be made applicable by contract or other legally binding action to contractors whenever a DCAA contract provides for the operation of a system of records or portion of a system of records to accomplish an agency function.

§ 317.3 Definitions.

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

(b) *Agency.* For the purposes of disclosing records subject to the Privacy Act among DoD components, the Department of Defense is considered a single agency. For all other purposes to include applications for access and amendment, denial of access or amendment, appeals from denials, and record-keeping as regards release to non-DoD agencies; each DoD component, including DCAA, is considered an agency within the meaning of the Privacy Act.

(c) *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 authority will be held in confidence or under an implied promise of such confidentiality if this implied promise was made before September 27, 1975.

(d) *Defense Data Integrity Board.* Consists of members of the Defense Privacy Board, as established pursuant to 32 CFR part 310, and in addition the Inspector General, DoD or the designee, when convening to oversee, coordinate and approve or disapprove all DoD component computer matching covered by the Privacy Act.

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

(f) *Federal benefit program.* Any program administered or funded by the Federal Government, or by any agent or state on behalf of the Federal Government, providing cash or in-kind as-

sistance in the form of payments, grants, loans, or loan guarantees to individuals.

(g) *Federal benefit program match.* A computerized comparison of two or more automated systems of records or an automated system of records with automated non-Federal records for the purpose of establishing or verifying the eligibility of or continuing compliance with statutory and regulatory requirements by, applicants for, recipients and beneficiaries (both present and past) of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs; or recouping payments or delinquent debts under such Federal benefit programs.

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

(i) *Federal personnel match.* A computerized comparison of two or more automated Federal personnel or payroll systems of records or an automated Federal personnel or payroll system of records with automated non-Federal records.

(j) *Individual.* A living citizen of the United States or an alien lawfully admitted to the United States for permanent residence. The legal guardian of an individual has the same rights as the individual and may act on his or her behalf. No rights are vested in the representative of a dead person under this chapter and the term "individual" does not embrace an individual acting in an interpersonal capacity (for example, sole proprietorship or partnership).

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

(l) *Maintain.* Includes maintain, collect, use, or disseminate.

(m) *Matching agency.* The agency which actually performs the match.

§317.3

32 CFR Ch. I (7-1-99 Edition)

(n) *Matching program.* (1) The term means any computerized comparison of:

(i) Two or more automated systems of records or a system of records with non-Federal records for the purpose of:

(A) Establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or

(B) Recouping payments or delinquent debts under such Federal benefit programs, or

(ii) Two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with non-Federal records,

(iii) But does not include:

(A) Matches performed to produce aggregate statistical data without any personal identifiers.

(B) Matches performed to support any research for statistical project, the specific data of which may not be used to make decisions concerning the rights, benefits, or privileges of specific individuals.

(C) Matches performed by an agency which performs as its principal function any activity pertaining to the enforcement of criminal laws, subsequent to the initiation of a specific criminal or civil law enforcement investigation of a named person or persons for the purpose of gathering evidence against such person or persons.

(iv) Matches of tax information.

(A) Pursuant to section 6103(d) of the Internal Revenue Code of 1986.

(B) For purposes of tax administration as defined in section 6301(b)(4) of such Code.

(C) For the purpose of intercepting a tax refund due an individual under authority granted by section 464 or 1137 of the Social Security Act; or

(D) For the purpose of intercepting a tax refund due an individual under any other tax refund intercept program authorized by statute which has been determined by the Director of the Office of Management and Budget to contain verification, notice, and hearing requirements that are substantially simi-

lar to the procedures in section 1137 of the Social Security Act.

(E) *Matches.* (1) Using records predominantly relating to Federal personnel, that are performed for routine administrative purposes (subject to guidance provided by the Director of the Office of Management and Budget pursuant to subsection (v) of the Privacy Act).

(2) Conducted by an agency using only records from systems of records maintained by that agency; if the purpose of the match is not to take any adverse financial, personnel, disciplinary, or other adverse action against Federal personnel; or

(F) Matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of Federal personnel or Federal contractor personnel.

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

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

(q) *Official use.* Within the context of this chapter, this term is used when officials and employees of the Agency have a demonstrated need for the use of any record or the information contained therein in the performance of their official duties, subject to DCAA Regulation 5410.10.

(r) *Personal information.* Information about an individual that is intimate or private to the individual, as distinguished from information related solely to the individual's official functions or public life.

(s) *Privacy Act.* The Privacy Act of 1974 (5 U.S.C. 552a), as amended.

(t) *Privacy Act request.* A request from an individual for notification as to the existence of, access to, or amendment of records pertaining to that individual. These records must be maintained in a system of records. The request must indicate that it is being made under the Privacy Act to be considered a Privacy Act request.

(u) *Recipient agency.* Any agency, or contractor thereof, receiving records

contained in a system of records from a source agency for use in a matching program.

(v) *Record.* Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, the individual's education, financial transactions, medical history, and criminal or employment history, and that contains the individual's name, or identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

(w) *Risk assessment.* An analysis considering information sensitivity, vulnerabilities, and the cost to a computer facility or word processing activity in safeguarding personal information processed or stored in the facility or activity. Applies to manual and automated systems.

(x) *Routine use.* The disclosure of a record outside the Agency for a use that is compatible with the purpose for which the information was collected and maintained by the Agency. The routine use must be included in the published system notice for the system of records involved.

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

(z) *Statistical record.* A record maintained only for statistical research or reporting purposes and not used in whole or in part in making determinations about specific individuals.

(aa) *System of records.* A group of records under the control of the Agency from which information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to the individual. System notices for all Privacy Act systems of records must be published in the FEDERAL REGISTER.

(bb) *Word processing equipment.* Any combination of electronic hardware and computer software integrated in a variety of forms (programmable software, hard wiring, or similar equip-

ment) that permits the processing of textual data.

(cc) *Word processing system.* A combination of equipment employing automated technology, systematic procedures, and trained personnel for the primary purpose of manipulating human thoughts and verbal or written communications into a form suitable to the originator.

§317.4 Policy.

It is DCAA policy that personnel will comply with the DCAA Privacy Program and the Privacy Act of 1974. Strict adherence is necessary to ensure uniformity in the implementation of the DCAA Privacy Program and create conditions that will foster public trust. It is also agency policy to safeguard personal information contained in any system of records maintained by DCAA organizational elements and to make that information available to the individual to whom it pertains to the maximum extent practicable. DCAA policy specifically requires that DCAA organizational elements:

(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 of Department of Defense; and

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

(d) Ensure that records used in making determinations about individuals and those containing personal information are accurate, relevant, timely, and complete for the purposes for which they are being maintained before making them available to any recipients

§317.5

outside of Department of Defense, other than a Federal agency, unless the disclosure is made under DCAA Regulation 5410.10, DCAA Freedom of Information Act Program (32 CFR part 290).

(e) Keep no record that describes how individuals exercise their rights guaranteed by the First Amendment to the U.S. Constitution, unless expressly authorized by statute or by the individual to whom the records pertain or is pertinent to and within the scope of an authorized law enforcement activity.

(f) Notify individuals whenever records pertaining to them are made available under compulsory legal processes, if such process is a matter of public record.

(g) Establish safeguards to ensure the security of personal information and to protect this information from threats or hazards that might result in substantial harm, embarrassment, inconvenience, or unfairness to the individual.

(h) Establish rules of conduct for DCAA personnel involved in the design, development, operation, or maintenance of any system of records and train them in these rules of conduct.

(i) Assist individuals in determining what records pertaining to them are being collected, maintained, used, or disseminated.

(j) Permit individual access to the information pertaining to them maintained in any system of records, and to correct or amend that information, unless an exemption for the system has been properly established for an important public purpose.

(k) Provide, on request, an accounting of all disclosures of the information pertaining to them except when disclosures are made:

(1) To DoD personnel in the course of their official duties.

(2) Under 32 CFR part 290; and

(3) To another agency or to an instrumentality of any governmental jurisdiction within or under control of the United States conducting law enforcement activities authorized by law.

(l) Advise individuals on their rights to appeal any refusal to grant access to or amend any record pertaining to them, and file a statement of disagree-

32 CFR Ch. I (7-1-99 Edition)

ment with the record in the event amendment is refused.

§317.5 Responsibilities.

(a) *Headquarters.* (1) The *Assistant Director, Resources* has overall responsibility for the DCAA Privacy Act Program and will serve as the sole appellate authority for appeals to decisions of respective initial denial authorities. Under his direction, the *Chief, Information Resources Management Branch*, under the supervision of the *Chief, Administrative Management Division* shall:

(i) Establish, issue, and update policies for the DCAA Privacy Act Program; monitor compliance with this part; and provide policy guidance for the DCAA Privacy Act Program.

(ii) Resolve conflicts that may arise regarding implementation of DCAA Privacy Act policy.

(iii) Designate an agency Privacy Act Advisor, as a single point of contact, to coordinate on matters concerning Privacy Act policy.

(iv) Make the initial determination to deny an individual's written Privacy Act request for access to or amendment of documents filed in Privacy Act systems of records. This authority cannot be delegated.

(2) The *DCAA Privacy Act Advisor* under the supervision of the *Chief, Information Resources Management Branch* shall:

(i) Manage the DCAA Privacy Act Program in accordance with this part and applicable DCAA policies, as well as Department of Defense and Federal regulations.

(ii) Provide guidelines for managing, administering, and implementing the DCAA Privacy Act Program.

(iii) Implement and administer the Privacy Act program at the Headquarters.

(iv) Ensure that the collection, maintenance, use, or dissemination of records of identifiable personal information is in a manner that assures that such action is for a necessary and lawful purpose; that the information is timely and accurate for its intended use; and that adequate safeguards are provided to prevent misuse of such information.

(v) Maintain and publish DCAA Pamphlet 5410.13⁴, "DCAA Compilation of Privacy Act System Notices"; DCAA Pamphlet 5410.15⁵, "Privacy Act of 1974, An Employee Guide to Privacy"; and DCAA Manual 5410.16, "DCAA Privacy Act Processing Guide."

(vi) Prepare promptly any required new, amended, or altered system notices for systems of records subject to the Privacy Act and submit them to the Defense Privacy Office for subsequent publication in the FEDERAL REGISTER.

(vii) Prepare the annual Privacy Act Report as required by 32 CFR part 310, "DoD Privacy Act Program."

(viii) Conduct training on the Privacy Act program for agency personnel.

(3) *Heads of Principal Staff Elements* are responsible for:

(i) Reviewing all regulations or other policy and guidance issuances for which they are the proponent to ensure consistency with the provisions of this part.

(ii) Ensuring that the provisions of this part are followed in processing requests for records.

(iii) Forwarding to the DCAA Privacy Act Advisor, any Privacy Act requests received directly from a member of the public, so that the request may be administratively controlled and processed.

(iv) Ensuring the prompt review of all Privacy Act requests, and when required, coordinating those requests with other organizational elements.

(v) Providing recommendations to the DCAA Privacy Act Advisor regarding the releasability of DCAA records to members of the public, along with the responsive documents.

(vi) Providing the appropriate documents, along with a written justification for any denial, in whole or in part, of a request for records to the DCAA Privacy Act Advisor. Those portions to be excised should be bracketed in red pencil, and the specific exemption or exemptions cited which provide the basis for denying the requested records.

(4) The *General Counsel* is responsible for:

(i) Ensuring uniformity is maintained in the legal position, and the interpretation of the Privacy Act (32 CFR part 310), and this part.

(ii) Consulting with General Counsel, Department of Defense on final denials that are inconsistent with decisions of other DoD components, involve issues not previously resolved, or raise new or significant legal issues of potential significance to other Government agencies.

(iii) Providing advice and assistance to the Assistant Director, Resources; Regional Directors; and the Regional Privacy Act Officer, through the DCAA Privacy Act Advisor, as required, in the discharge of their responsibilities.

(iv) Coordinating Privacy Act litigation with the Department of Justice.

(v) Coordinating on Headquarters denials of initial requests.

(5) Each *Regional Director* is responsible for the overall management of the Privacy Act program within their respective regions. Under his/her direction, the *Regional Resources Manager* is responsible for the management and staff supervision of the program and for designating a *Regional Privacy Act Officer*.

(i) *Regional Directors* will, as designee of the Director, make the initial determination to deny an individual's written Privacy Act request for access to or amendment of documents filed in Privacy Act systems of records. This authority cannot be delegated.

(ii) *Regional Privacy Act Officers* will:

(A) Implement and administer the Privacy Act program throughout the region.

(B) Ensure that the collection, maintenance, use, or dissemination of records of identifiable personal information is in a manner that assures that such action is for a necessary and lawful purpose; that the information is timely and accurate for its intended use; and that adequate safeguards are provided to prevent misuse of such information.

(C) Prepare input for the annual Privacy Act Report as shown in DCAA Manual 5410.16 when requested by the DCAA Information and Privacy Advisor.

⁴See footnote 1 to §317.1(a).

⁵See footnote 1 to §317.1(a).

§317.6

(D) Conduct training on the Privacy Act program for regional and FAO personnel.

(E) Provide recommendations to the Regional Director through the Regional Resources Manager regarding the releasability of DCAA records to members of the public.

(6) *Managers, Field Audit Offices (FAOs)* will:

(i) Ensure that the provisions of this part are followed in processing requests for records.

(ii) Forward to the Regional Privacy Act Officer, any Privacy Act requests received directly from a member of the public, so that the request may be administratively controlled and processed.

(iii) Ensure the prompt review of all Privacy Act requests, and when required, coordinating those requests with other organizational elements.

(iv) Provide recommendations to the Regional Privacy Act Officer regarding the releasability of DCAA records to members of the public, along with the responsive documents.

(v) Provide the appropriate documents, along with a written justification for any denial, in whole or in part, of a request for records to the Regional Privacy Act Officer. Those portions to be excised should be bracketed in red pencil, and the specific exemption or exemptions cited which provide the basis for denying the requested records.

(7) *DCAA Employees* will:

(i) Not disclose any personal information contained in any system of records, except as authorized by this part.

(ii) Not maintain any official files which are retrieved by name or other personal identifier without first ensuring that a notice for the system has been published in the FEDERAL REGISTER.

(iii) Report any disclosures of personal information from a system of records or the maintenance of any system of records that are not authorized by this part to the appropriate Privacy Act officials for their action.

§317.6 Procedures.

Procedures for processing material in accordance with the Privacy Act of

32 CFR Ch. I (7-1-99 Edition)

1974 are outlined in subparts B through L of this part.

Subpart B—Systems of Records

§317.10 General.

(a) *System of records.* To be subject to this part, a "system of records" must:

(1) Consist of "records" that are retrieved by the name or some other personal identifier of an individual, and

(2) Be under the control of the Agency.

(b) *Retrieval practices.* (1) Records in a group of records that could be retrieved by personal identifiers, but are not covered by this part, even if the records contain information about individuals and are under the control of the agency. The records must, in fact, be retrieved by personal identifiers in order to become a system of records.

(2) If records previously not retrieved by personal identifiers are rearranged so they are retrieved by personal identifiers, a new system of records is created and a notice of the system must be published in the FEDERAL REGISTER of its existence.

(3) If records in a system of records are rearranged so retrieval no longer is by personal identifiers, the records are no longer subject to this part and the records system notice shall be deleted.

(c) *Recordkeeping standards.* A record maintained in a system of records must meet the following criteria:

(1) The record must be accurate--all information in the record must be factually correct.

(2) The record must be relevant--all information contained in the record must be related to the individual who is the subject of record and also must be related to a lawful purpose or mission of the agency.

(3) The record must be timely--all information in the record must be reviewed periodically to ensure that it has not changed due to time or later events.

(4) The record must be complete--it must be able to stand alone in accomplishing the purpose for which it is maintained.

(5) The record must be necessary--all information in the record must be

needed to accomplish the agency mission or purpose established by Federal law or Executive Order of the President.

(d) *Authority to establish systems of records.* The specific Federal statute or Executive Order of the President should be identified that authorizes maintaining each system of records. A statute or Executive Order authorizing a system of records does not negate the responsibility to ensure the information in the system of records is relevant and necessary.

(e) *Exercise of first amendment rights.*

(1) Records should not be maintained describing how an individual exercises rights guaranteed by the first amendment of the U.S. Constitution unless:

(i) Expressly authorized by Federal law;

(ii) Expressly authorized by the individual; or

(iii) Pertinent to and within the scope of an authorized law enforcement activity.

(2) First amendment rights include, but are not limited to, freedom of religion, freedom of political beliefs, freedom of speech, freedom of the press, the right to assemble, and the right to petition.

(f) *System manager's evaluations and reviews.* (1) Each new proposed system of records shall be evaluated.

(i) The information to be included in the system should be evaluated before establishing it.

(ii) The following factors should be considered:

(A) The relationship of each item of information to be collected and retained to the purpose for which the system is maintained. All information must be relevant to the purpose.

(B) The specific impact on the purpose or mission if each category of information is not collected. All information must be necessary to accomplish a lawful purpose or mission.

(C) The ability to meet the informational needs without using personal identifiers (will anonymous statistical records meet the needs?).

(D) The length of time each item of information must be kept.

(E) The methods of disposal; and

(F) The cost of maintaining the information.

(2) All existing systems of records shall be evaluated and reviewed.

(i) When an alteration or amendment of an existing system is prepared, an evaluation must be performed.

(ii) Reviews should be conducted often and reports prepared which outline the results and corrective actions taken to resolve problems uncovered.

(A) Training practices should be reviewed annually to ensure all personnel are familiar with the requirements of the Privacy Act and any special needs their specific jobs entail.

(B) Recordkeeping and disposal practices should be reviewed annually to ensure compliance with this part.

(C) Each ongoing computer matching program in which records from the system have been matched with non-DoD records should be reviewed annually to ensure that the applicable requirements have been met.

(D) Actions of agency personnel that resulted in either the agency being found civilly liable or an employee being found criminally liable should be reviewed annually to determine the extent of the problem and find the most effective way of preventing the problem in the future.

(E) Each system of records notice should be reviewed annually to ensure it accurately describes the system. Where minor changes are needed, amend the system notice. If major changes are needed, alter the system notice.

(F) A random sample of agency contracts that provide for the operation of a system of records on behalf of the agency to accomplish an agency function should be reviewed every even-numbered year to ensure the wording of each contract complies with the provisions of the Privacy Act of 1974 (5 U.S.C. 552a).

(G) The routine use disclosures associated with each system of records should be reviewed every three years to ensure the recipient's use of the records continues to be compatible with the purpose for which the agency originally collected the information.

(H) Each system of records for which exemption rules have been established should be reviewed every three years to determine whether each exemption is still needed.

§317.11

(iii) When directed, the reports should be sent through proper channels to the agency Privacy Act Advisor who will forward them to the Defense Privacy Office.

(g) *Discontinued information requirements.* (1) Any category or item of information about individuals that is no longer justified should not be collected, and when feasible, the information should be removed from existing records.

(2) Records that must be kept in accordance with retention and disposal needs established under DCAA Manual 5015.1⁶, "Files and Disposition Manual," shall not be destroyed.

(h) *Review records before disclosing them outside the Federal government.* Before disclosing a record from a system of records to anyone outside the Federal government, reasonable steps should be taken to ensure the record to be disclosed is accurate, relevant, timely, and complete for the purposes it is being maintained.

§317.11 Federal Government contractors.

(a) *Applicability to Federal government contractors.* (1) When the agency contracts for the operation of a system of records or portion thereof to accomplish an agency function, this part and 5 U.S.C. 552a are applicable. For purposes of the criminal penalties, the contractor and its employees shall be considered employees of the agency during the performance of the contract.

(2) Consistent with Parts 24 and 52 of the Federal Acquisition Regulation⁷, contracts for the operation of a system of records or portion thereof shall identify specifically the record system and the work to be performed, and shall include in the solicitations and resulting contract such terms specifically prescribed by the FAR.

(3) If the contractor must use records that are subject to this part to perform any part of a contract, and the information would have been collected and maintained by the agency but for the

⁶See footnote 1 to §317.1(a).

⁷For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402.

32 CFR Ch. I (7-1-99 Edition)

contract, the contractor activities are subject to this rule.

(4) This rule does not apply to records of a contractor that are:

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

(ii) Maintained as internal contractor employee records, even when used in conjunction with providing goods or services to the agency.

(iii) For contracting that is subject to this part, the agency shall:

(A) Inform prospective contractors of their responsibilities under the DCAA Privacy Program.

(B) Establish an internal system for reviewing contractor performance to ensure compliance with the DCAA Privacy Program; and

(C) Provide for the biennial review of a random sampling of agency contracts that are subject to this rule.

(b) *Contracting procedures.* The Defense Acquisition Regulatory Council is responsible for developing the specific policies and procedures for soliciting, awarding, and administering contracts.

(c) *Contractor compliance.* The agency shall establish contract surveillance programs to ensure contractors comply with the procedures established by the Defense Acquisition Regulatory Council pursuant to the preceding subsection.

(d) *Disclosing records to contractors.* Disclosing records to a contractor for use in performing a contract for the agency is considered a disclosure within the agency. The contractor is considered the agent of DCAA when receiving and maintaining the records for the agency.

§317.12 Safeguarding information in systems of records.

(a) *General responsibilities.* Appropriate administrative, technical, and physical safeguards shall be established to ensure the records in every system of records are protected from unauthorized alteration, destruction, or disclosure. The records shall be protected from reasonably anticipated

threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

(b) *Minimum standards.* (1) Risk analysis and management planning shall be conducted for each system of records. Sensitivity and use of the records, present and projected threats and vulnerabilities, and present and projected cost-effectiveness of safeguards should be considered. The risk analysis may vary from an informal review of a small, relatively insensitive system to a formal, fully quantified risk analysis of a large, complex, and highly sensitive system.

(2) All personnel operating a system of records or using records from a system of records should be trained in proper record security procedures.

(3) Information exempt from disclosure under DCAA Freedom of Information Act Program (32 CFR part 290), shall be labeled to reflect its sensitivity, such as "FOR OFFICIAL USE ONLY," "PRIVACY ACT SENSITIVE: DISCLOSE ON A NEED-TO-KNOW BASIS ONLY," or some other language that alerts individuals to the sensitivity of the records.

(4) Special administrative, physical, and technical safeguards shall be employed to protect records stored or processed in an automated data processing or word processing system from threats unique to those environments.

(c) *Records disposal.* (1) Records from systems of records should be disposed of to prevent inadvertent disclosure. Disposal methods such as tearing, burning, melting, chemical decomposition, burying, pulping, pulverizing, shredding, or mutilation are considered adequate if the records are rendered unrecognizable or beyond reconstruction. Magnetic media may be cleared by degaussing, overwriting, or completely erasing.

(2) The transfer of large volumes of records (e.g., computer cards and printouts) in bulk to a disposal activity such as a Defense Reutilization and Marketing Office for authorized disposal is not a disclosure of records under this rule if volume of the records, coding of the information, or some other factor renders it impossible

to recognize any personal information about a specific individual.

(3) When disposing or destroying large quantities of records from a system of records, care must be taken to ensure that the bulk of the records is maintained to prevent easy identification of specific records. If such bulk is maintained, no special procedures are required. If bulk is not maintained, or if the form of the records makes individually identifiable information easily discernible, dispose of the records in accordance with paragraph (c)(1) of this section.

Subpart C—Collecting Information About Individuals

§ 317.20 General considerations.

(a) *Collect directly from the individual.* To the greatest extent practicable, information should be collected for systems of records directly from the individual to whom the record pertains if the record may be used to make an adverse determination about the individual's rights, benefits, or privileges under Federal programs.

(b) *Soliciting the Social Security number.* (1) It is unlawful for any Federal, State, or local government agency to deny an individual a right, benefit, or privilege provided by law because the individual refuses to provide the Social Security Number (SSN). However, this prohibition does not apply if:

(i) A Federal law requires that the SSN be provided, or

(ii) The SSN is required by a law or regulation adopted before January 1, 1975, to verify the individual's identity for a system of records established and in use before that date.

(2) Before requesting an individual to provide the SSN, the individual shall be told:

(i) Whether providing the SSN is voluntary or mandatory,

(ii) By what law or other authority the SSN is solicited, and

(iii) What uses will be made of the SSN.

(3) The notice published in the FEDERAL REGISTER for each system of records containing SSNs solicited from individuals must indicate the authority for soliciting the SSNs and whether

§317.21

32 CFR Ch. I (7–1–99 Edition)

it is mandatory for the individuals to provide their SSNs. Executive Order 9397 permits Federal agencies to solicit SSNs as numerical identifiers for individuals in Federal records systems.

(4) Upon entrance into employment with the agency, individuals must provide their SSNs; therefore, they must be given the notification. The SSN is then the individual's numerical identifier and used to establish personnel, financial, medical, and other official records. After the individual has provided the SSN to establish the records, the notification is not required when the SSN is requested only for verification or to locate the records.

(5) The Federal Personnel Manual should be consulted when soliciting SSNs for use in systems of records controlled by the Office of Personnel Management.

(c) *Collecting information about individuals from third persons.* It might not always be practical to collect all information about the individual directly from the individual, such as when:

(1) Verifying information through other sources for security or employment suitability determinations.

(2) Seeking other opinions, such as a supervisor's comments on past performance or other evaluations.

(3) Obtaining the necessary information directly from the individual will be exceptionally difficult or will result in unreasonable costs or delays; or

(4) The individual requests or consents to contacting another person to obtain the information.

(d) *Privacy Act statement.* (1) When an individual is requested to furnish information about himself or herself for a system of records, a Privacy Act statement must be provided to the individual, regardless of the method used to collect the information (forms, personal interviews, telephonic interviews, etc.). If the information requested will not be included in a system of records, a Privacy Act statement is not required.

(2) The Privacy Act statement shall include the following:

(i) The Federal law or Executive Order of the President that authorizes collecting the information.

(ii) Whether it is voluntary or mandatory for the individual to provide the requested information.

(iii) The principal purposes for which the information will be used.

(iv) The routine uses that will be made of the information (to whom and why it will be disclosed outside the Department of Defense); and

(v) The effects, if any, on the individual if all or part of the information is not provided.

(3) The Privacy Act statement must appear on the form used to collect the information or on a separate form that can be retained by the individual requesting it. If the information is collected other than by the individual completing a form, such as when the information is solicited by telephone, the Privacy Act statement should be read to the individual and a copy sent to him or her on request.

(4) It is mandatory for an individual to furnish information about himself or herself for a system of records only when a Federal law or Executive Order of the President specifically imposes a duty to furnish the information and provides a penalty, e.g., criminal sanctions, for failure to do so. If furnishing the information is only a condition for granting a benefit or privilege voluntarily sought by the individual (such as a request for annual leave), it is voluntary for the individual to give the information. However, the denial of the benefit or privilege must be listed in the Privacy Act statement as one of the effects of not providing the information, i.e., the effects on the individual if the information is not provided.

§317.21 Forms.

(a) *DCAA forms.* (1) DCAA Regulation 5015.3⁸, "DCAA Forms Management Program," provides guidance for preparing the Privacy Act statement for use with DCAA forms.

⁸Copies may be obtained, at cost, from the Defense Contract Audit Agency, ATTN: CMO, Cameron Station, Alexandria, VA 22304-6178.

(2) When forms are used to collect information about individuals for a system of records, the Privacy Act statement shall appear as follows (listed in the order of preference):

(i) Immediately below the title of the form.

(ii) Elsewhere on the front page of the form (clearly indicating it is the Privacy Act statement).

(iii) On the back of the form with a notation of its location below the title of the form, or

(iv) On a separate form which the individual may keep.

(b) *Non-DCAA forms.* Forms subject to 5 U.S.C. 552a issued by other DoD components or Federal agencies might contain a Privacy Act statement; however, the statement might not reflect accurately the authority, purposes, and routine uses applicable within the agency. If so, the activity using the form shall prepare a statement or supplement to the one provided with the form.

Subpart D—Access to Records

§ 317.30 Individual access to records.

(a) *Right of access* (1) The access provisions of this part are for individuals who are subjects of records maintained in DCAA systems of records.

(2) All information that can be released consistent with applicable laws and regulations should be made available to the subject of record.

(b) *Notification of record's existence.* Record managers of system of records shall establish procedures for notifying an individual, in response to a request, if the system of records contains a record pertaining to him or her.

(c) *Individual requests for access.* (1) Individuals shall address requests for access to records in systems of records to the responsible system manager or the regional Privacy Act officer.

(2) Requests for access may be oral or written; however, only written requests are to be maintained in the Privacy Act case file and counted when compiling the annual Privacy Act report.

(d) *Verifying identity.* (1) An individual shall provide reasonable

verification of identity before obtaining access to records.

(2) Procedures for verifying identity shall not be complicated merely to discourage individuals from seeking access to records.

(3) When an individual seeks access in person, identification can be verified by documents normally carried by the individual, such as an identification card, driver's license, or other license, permit or pass normally used for identification purposes.

(4) When access is requested other than in person, identity may be verified by the individual's providing minimum identifying data such as full name, date and place of birth, or other information necessary to locate the record sought. If the information sought is sensitive, additional identifying data may be required.

(5) The individual may be accompanied by a person of his or her choice when viewing the record; however, the individual may be required to provide written authorization to have the record discussed in front of the other person.

(6) An individual shall not be denied access to a record solely for refusing to divulge the SSN, unless it is the only means of retrieving the record or verifying identity.

(7) An individual shall not be required to explain why he or she is seeking access to a record.

(8) Only a designated denial authority may deny access. The denial must be in writing.

(9) If notarization of requests is required for access, procedures shall be established for an alternate method of verification for individuals who do not have access to notary services, such as military members overseas. The following formats may be used as prescribed by 28 U.S.C. 1746:

(i) If executed outside of 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*

§ 317.30

32 CFR Ch. I (7-1-99 Edition)

that the foregoing is true and correct. Executed on (date). (Signature)."

(e) *Granting individual access to records.* (1) The individual should be granted access to the original record (or exact copy) without any changes or deletions. A record that has been amended is considered the original.

(2) The individual's request should be granted for an exact copy of the record, and, upon the signed authorization of the individual, a copy should be provided to anyone designated by the individual. In either case, the copying fees may be assessed to the individual.

(3) If requested, explain any record or portion of a record that is not understood, as well as any changes or deletions.

(f) *Illegible, incomplete, or exempt records.* (1) Illegible or incomplete records. Individual access should not be denied solely because the physical condition or format of the record does not make it readily available, such as when the record is in a deteriorated state or on magnetic tape. In this case, the document should be recopied exactly or an extract can be prepared.

(2) Exempt records. A request for a record that is wholly or partially exempt from access shall also be processed under the Freedom of Information Act (FOIA). The requester shall be granted access to all information that is releasable under either this part or the FOIA. The agency may provide this information in the form of an extract or summary of the record. The provisions of this rule or the FOIA under which access was granted should be cited.

(g) *Access to medical and psychological records.* (1) Individual access to medical and psychological records should be provided, even if the individual is a minor, unless it is determined that access could have an adverse effect on the mental or physical health of the individual. This determination normally should be made in consultation with a medical practitioner.

(2) If it is medically indicated that access could have an adverse mental or physical effect on the individual, the record should be provided to a medical practitioner named by the individual, along with an explanation why access

without medical supervision could be harmful to the individual.

(3) The named medical practitioner should not be required to request the record for the individual.

(4) If the individual refuses or fails to designate a medical practitioner, access shall be refused. The refusal is not considered a denial for reporting purposes under the Privacy Act.

(h) *Access by parents and legal guardians.* (1) The parent of any minor, an individual under 18 years of age who is neither a member of a Military Service nor married, or the legal guardian of any individual declared by a court of competent jurisdiction to be incompetent due to physical or mental incapacity or age, may obtain access to the record of the minor or incompetent individual if the parent or legal guardian is acting on behalf of the minor or incompetent (i.e., for the benefit of the minor or incompetent). However, with respect to access by parents and legal guardians to medical records and medical determinations about minors, observe the following procedures:

(i) In the United States, the laws of the state where the records are located might afford special protection to certain medical records such as drug and alcohol abuse treatment records and psychiatric records. The state statutes might apply even if the records are maintained by a military medical facility.

(ii) For installations located outside the United States, the parent or legal guardian of a minor shall be denied access if all four of the following conditions are met:

(A) The minor at the time of the treatment or consultation was 15, 16, or 17 years old.

(B) The treatment or consultation was within a program authorized by law or regulation to provide confidentiality to the minor.

(C) The minor specifically indicated a desire that the treatment or consultation record be handled in confidence and not disclosed to a parent or guardian, and

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

(2) A minor or incompetent has the same right of access as any other individual. The right of access of the parent or legal guardian is in addition to that of the minor or incompetent.

(i) *Access to information compiled in anticipation of a civil proceeding.* (1) An individual is not entitled to access information compiled in reasonable anticipation of a civil action or proceeding.

(2) The term "civil action or proceeding" includes quasi-judicial and pretrial judicial proceedings as well as formal litigation.

(3) Paragraphs (i)(1) and (2) of this section do not prohibit access to records compiled or used for purposes other than litigation, nor prohibit access to systems of records solely because they are frequently subject to litigation. The information must have been compiled for the primary purpose of litigation.

(4) Attorney work products prepared in conjunction with the paragraphs (i)(1) and (2) of this section are also protected.

(j) *Non-agency records.* (1) Certain documents under the control of DCAA personnel and used to assist them in performing official functions may not be considered agency records within the meaning of this part. Such documents, if maintained in accordance with the following subparagraph, are not systems of records that are subject to this part. Examples are personal telephone lists and personal notes kept to refresh the memory of the author.

(2) To be considered non-agency records, the documents must:

(i) Be maintained and discarded solely at the discretion of the author.

(ii) Be created only for the author's personal convenience.

(iii) Not be the result of official direction or encouragement, whether oral or written; and

(iv) Not be shown to other persons for any reason.

(k) *Relationship between the Privacy Act and the Freedom of Information Act (FOIA).* (1) Access requests that specifically state or reasonably imply that they are made under the Freedom of Information Act (5 U.S.C. 552), are processed pursuant to DCAA Regulation 5410.10 (32 CFR part 290).

(2) Access requests that specifically state or reasonably imply that they are made under the Privacy Act of 1974 (5 U.S.C. 552a) are processed pursuant to this part.

(3) Access requests that cite both the FOIA and the Privacy Act are processed under the Act that provides the greater degree of access. The requester should be informed which Act was used in granting or denying access.

(4) Individual access should not be denied to records otherwise releasable under the Privacy Act or the Freedom of Information Act solely because the request does not cite the appropriate statute.

(l) *Time limits.* Access requests should be acknowledged within 10 working days after receipt, and access should be granted or denied within 30 working days, excluding Federal holidays.

§ 317.31 Reproduction fees.

(a) *Fee schedules.* The fees charged requesters shall include only the direct cost of reproduction and shall not include costs of:

(1) Time or effort devoted by agency personnel to searching for or reviewing the record.

(2) Fees not associated with the actual cost of reproduction.

(3) Producing a copy when it must be provided to the individual without cost under another regulation, directive, or law.

(4) Normal postage.

(5) Transportation of records or personnel, or

(6) Producing a copy when the individual has requested only to review the record and has not requested a copy to keep, and

(i) The only means of allowing review is to make a copy (e.g., the record is stored in a computer and a copy must be printed to provide individual access), or

(ii) The agency does not wish to surrender temporarily the original record for the individual to review.

(7) Compute fees using the appropriate portions of the fee schedule in 32 CFR part 286, subpart F.

(b) *Fee waivers.* (1) Fees shall be waived automatically if the direct cost of reproduction is less than \$30, unless the individual is requesting an obvious

§ 317.32

extension or duplication of a previous request for which he or she was granted a waiver.

(2) Decisions to waive or reduce fees that exceed \$30 may be made on a case-by-case basis.

§ 317.32 Denying individual access.

(a) *Denying individual access.* The subject of record may be denied access only if it:

(1) Was compiled in reasonable anticipation of a civil action or proceeding; or

(2) Is in a system of records that has been exempted from the access provisions of this part.

(3) The individual should be denied access only to those portions of the record for which the denial will serve a legitimate governmental purpose.

(4) An individual may be refused access for failure to comply with established procedural requirements, but must be told the specific reason for the refusal and the proper access procedures.

(b) *Notifying the individual.* Written denial of access must be given to the individual and must be documented in a Privacy Act case file. The denial shall include:

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

(2) The date of the denial.

(3) The specific reason for the denial, citing the appropriate sections of the Privacy Act or this part authorizing the denial.

(4) Notice of the individual's right to appeal the denial within 60 calendar days of the date the notice is mailed; and

(5) The title and address of the appeal official.

(c) *Appeal procedures.* Appeal procedures provide for the following:

(1) Review by the Assistant Director, Resources, DCAA Headquarters, or his or her designee, of any appeal by an individual.

(2) Written notification to the individual by the Assistant Director, Resources shall:

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

(A) The reason for denying the appeal, citing the provision of the Pri-

32 CFR Ch. I (7-1-99 Edition)

vacancy Act or this part upon which the denial is based.

(B) The date of the appeal determination.

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

(D) A statement informing the applicant of the right to seek judicial relief in Federal District Court.

(ii) If the appeal is granted, advise the individual and provide access to the record sought.

(d) *Final action, time limits, and documentation.* (1) The written appeal notification granting or denying access is the final agency action on the initial request for access.

(2) All appeals shall be processed within 30 working days, excluding Federal holidays, of receipt, unless the appeal authority finds that an adequate review cannot be completed within that period. If additional time is needed, notify the applicant in writing, explaining the reason for the delay and when the appeal will be completed.

(3) All actions on appeals must be documented in the Privacy Act case file.

(e) *Denial of appeal by the agency's failure to act.* An individual may consider his or her appeal denied if the appeal authority fails:

(1) To take final action on the appeal within 30 working days, excluding Federal holidays, of receipt when no extension of time notice was given; or

(2) To take final action within the period established by the extension of time notice.

(f) *Denying access to Office of Personnel Management (OPM) records held by the agency.* (1) The records in all systems of records maintained in accordance with the OPM Government-wide system notices are only in the temporary custody of the agency.

(2) All requests for access to these records must be processed in accordance with the OPM Federal Personnel Manual as well as DCAA Manual 1400.1⁹, "DCAA Personnel Management Manual."

⁹See footnote 1 to § 317.1(a).

(3) When DCAA initially denies access to a record in an OPM Government-wide system, the agency shall instruct the individual to direct any appeal to the Assistant Director for Workforce Information, Personnel Systems and Oversight Group, Office of Personnel Management, 1900 E Street, NW, Washington, DC 20415-0001.

§ 317.33 Privacy Act case files.

(a) Documents used in processing notification, access, and amendment requests made under the Privacy Act or this part shall be filed in a Privacy Act case file established for each request, not in the record to which they pertain.

(b) Privacy Act case files should contain the following information:

(1) The request to be notified if a system of records contains a record pertaining to the individual and the request for access and amendment.

(2) Approval, denial, request for appeal, action on appeal, coordination action, and other documents relating to the request; and

(3) Documentation of reasons for exceeding the established time limits for processing the request.

(c) The Privacy Act case file shall not contain a copy of the record and shall not be used to make any determination about the individual, other than determinations about the Privacy Act request.

(d) The case file shall be used only to process requests and provide statistics such as for the annual report required by the Privacy Act.

Subpart E—Amendment of Records

§ 317.40 Individual review and amendment.

Individuals are encouraged to review periodically the information maintained about them in systems of records, and to avail themselves of the amendment procedures established by this part.

§ 317.41 Amending records.

(a) *Right to request amendment.* An individual may request the amendment of any record retrieved by his or her

personal identifier from a system of records, unless the system has been exempted from the amendment procedures. See § 317.133. Amendments are limited to correcting factual matters, not matters of opinion such as those contained in evaluations of promotion potential and performance appraisals.

(b) *Written amendment request.* The agency may require that amendment requests be in writing; however, this requirement shall not be used merely to discourage individuals from requesting valid amendments or to burden needlessly the amendment process. Only written amendment requests must be documented in the Privacy Act case file.

(c) *Content of amendment request.* An amendment request must include:

(1) A description of the information to be amended.

(2) The reason for the amendment.

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

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

§ 317.42 Burden of proof.

The individual must provide adequate support for the request.

§ 317.43 Verifying identity.

The individual may be required to provide identification to prevent the inadvertent or intentional amendment of another's record.

§ 317.44 Limits on amending judicial and quasi-judicial evidence and findings.

This part does not permit the alteration of evidence presented in the course of judicial or quasi-judicial proceedings. Amendments to such records must be made in accordance with procedures established for such proceedings. This part does not permit a collateral attack on a judicial or quasi-judicial finding; however, it may be used to challenge the accuracy of recording the finding in a system of records.

§ 317.45

§ 317.45 Standards for amendment request determinations.

The record which the individual requests to be amended must meet agency recordkeeping standards. The record must be accurate, relevant, timely, complete, and necessary. If the record in its present state does not meet each of the criteria, the amendment request shall be granted to the extent necessary to meet them.

§ 317.46 Time limits.

Within 10 working days, excluding Federal holidays, of receiving an amendment request, provide the individual a written acknowledgment of the request. If action on the amendment request is completed within the 10 working days and the individual is so informed, no separate acknowledgment is necessary. The acknowledgment must clearly identify the request and advise the individual when to expect notification of the completed action. Only under exceptional circumstances shall more than 30 working days, excluding Federal holidays, be required to complete the action on an amendment request. If a completed action takes longer than 30 working days, the delay must be explained fully in the Privacy Act case file.

§ 317.47 Granting an amendment request in whole or in part.

(a) *Notify the requester.* To the extent the amendment request is granted, the individual shall be notified and make the appropriate amendment.

(b) *Notify previous recipients.* All previous recipients of the information (as reflected in the disclosure accounting records) should be notified that the amendment has been made and provide each a copy of the amended record. Recipients who are known to be no longer retaining the record need not be advised of the amendment. If it is known that other DoD components or other Federal Agencies have been provided the information that was amended, or if the individual requests that other DoD components or other Federal agencies be notified, provide the notification even if those components or agencies are not listed in the disclosure accounting.

32 CFR Ch. I (7–1–99 Edition)

(c) *Documentation.* The action should be documented in the Privacy Act case file if the request for amendment was in writing.

§ 317.48 Denying an amendment request in whole or in part.

(a) If the amendment request is denied in whole or in part, the individual should be promptly notified in writing and document the action in the Privacy Act case file. The notification to the individual shall include:

(b) *Basis for denial.* Those sections of the Privacy Act or this part upon which the denial is based.

(c) *Right to appeal.* Advice that the individual may appeal to the Assistant Director, Resources, or his or her designee for an independent review of the initial denial.

(d) *Appeal procedures.* The procedures for requesting an appeal, including the title and address of the official to whom the appeal should be sent; and

(e) *Appeal assistance.* Where the individual can receive assistance in filing the appeal.

§ 317.49 Appeal procedures.

Procedures to ensure the prompt, complete, and independent review of each denial of an amendment request if the individual appeals must ensure:

(a) *Appeals are forwarded.* The appeal with all supporting documentation, including that furnished by the individual and that contained in agency records, is provided to the Assistant Director, Resources, or his or her designee.

(b) *Standards for review.* The standard for deciding the appeal is whether the unamended record is accurate, relevant, timely, complete, and necessary. If the unamended record does not meet each of these criteria, the amendment request shall be granted to the extent necessary to meet them.

(c) *Time limits.* The appeal is processed within 30 working days, excluding Federal holidays, unless the appeal official determines that an adequate review cannot be completed within that period and gives the individual a written explanation of the reason and when the review will be completed.

(d) *Denial notification.* If the appeal is denied completely or in part, the individual is provided written notification that:

(1) The appeal has been denied, citing the sections of the Privacy Act or this rule on which the denial was based.

(2) The individual may file a statement of disagreement. An explanation of the filing procedures will be included in the written notification.

(3) If properly filed, the statement of disagreement shall be included in the record and furnished to all future recipients of the record and to all prior recipients of the record as listed on the disclosure accounting, except those known to be no longer retaining the record; and

(4) The individual may seek judicial review of the decision not to amend the record.

(e) *Amendment notification.* If the record is amended:

(1) The individual is notified promptly of the decision.

(2) All previous recipients of the record, as listed in the disclosure accounting (except those known to be no longer retaining the record), are notified of the amendment and provided a copy; and

(3) Any previous recipient known to be holding a copy of the record (but not listed in the disclosure accounting), as well as any other DoD component or other Federal agency named by the individual, also should be informed of the amendment and provided a copy.

(f) *Documentation.* All actions on the appeal shall be documented in the Privacy Act case file.

§ 317.50 Requests for amending OPM records.

The records in an OPM Government-wide system of records are only temporarily in the custody of the agency. Requests for amendment of these records must be processed in accordance with the OPM Federal Personnel Manual. The agency denial authority may deny a request, but all denials are subject to review by the Assistant Director for Workforce Information, Personnel Systems Oversight Group, Office of Personnel Management, 1900 E Street NW, Washington, DC 20415-0001.

§ 317.51 Individual's statement of disagreement.

(a) *Right to submit.* If the appeal authority refuses to amend the record as requested, the individual may submit a concise statement of disagreement listing the reasons for disagreeing with the refusal to amend.

(b) *Filing the statement.* If possible, incorporate the statement of disagreement into the record. If that is not possible, the record should be annotated to reflect that the statement was filed and maintain the statement so that it can be obtained readily when the disputed information is used or disclosed. For instance, automated record systems not programmed to accept statements of disagreement must be capable of having indicators entered to reflect the presence of statements on file and how to obtain them.

(c) *Inform previous recipients.* Copies of the statement of disagreement should be furnished to all individuals listed in the disclosure accounting of the record (except those known to be no longer retaining the record), as well as to all other known holders of copies of the record.

(d) *Disclosure.* Whenever the disputed information is disclosed for any purpose, ensure that the statement of disagreement also is used or disclosed.

§ 317.52 Agency's statement of reasons.

(a) *Right to file.* If the individual files a statement of disagreement, the agency may file a statement of reasons containing a concise summary of the agency's reasons for denying the amendment request.

(b) *Content.* The statement of reasons shall contain only those reasons given to the individual by the appeal official and shall not contain any comments on the individual's statement of disagreement.

(c) *Disclosure.* At the discretion of the agency, the statement of reasons may be disclosed to those individuals, DoD components, and other Federal agencies that receive the statement of disagreement.

Subpart F—Disclosure of Records**§ 317.60 Conditions of disclosure.**

(a) *Disclosures to third persons.* (1) Under the Privacy Act, there are two terms describing how information from a record is provided:

(i) “Access” occurs when information from a record is provided or shown to the individual who is the subject of record or, if that individual is a minor or incompetent, to the parent or legal guardian.

(ii) “Disclosure” occurs when information from a record is provided or shown to anyone other than the subject of record, or the parent or legal guardian of a minor or incompetent.

(b) *When disclosures may be made.* Disclosures may be made only when:

(1) The subject of record gives written consent for the disclosure; or

(2) One of the twelve conditions specified in § 317.61.

(c) *Validation before disclosure.* Except for disclosures made under the FOIA or DCAA Regulation 5410.10 (32 CFR part 290), make reasonable efforts to ensure the record is accurate, relevant, timely, and complete for agency purposes before disclosing any record from a system of records to any recipient other than a Federal agency. Records discovered to have been improperly filed in the system of records should be removed before disclosure.

(1) If validation cannot be obtained from the record itself, the agency may contact the subject of record (if reasonably available) to verify the accuracy, timeliness, completeness, and relevancy of the information.

(2) If validation cannot be obtained from the record and the subject of record is not reasonably available, the recipient should be advised that the information is believed to be valid as of a specific date and reveal any factors bearing on the validity of the information.

§ 317.61 Non-consensual disclosures.

The Privacy Act provides twelve instances when a record in a system of records may be disclosed without the written consent of the subject of the record:

(a) *Disclosures within the Department of Defense for official purposes.* For purposes of disclosing records among DoD components, the Department of Defense is considered a single agency; hence, a record may be disclosed to any officer or employee in the Department of Defense who needs it in the performance of official duties. Rank or position alone does not authorize the disclosure; there must be a demonstrated official need.

(b) *Disclosures required by the Freedom of Information Act (FOIA).* (1) A record must be disclosed if required by the FOIA, which is implemented by DCAA Regulation 5410.10 (32 CFR part 290).

(2) The FOIA requires that records be made available to any person requesting them in writing, unless the record is exempt from disclosure under one of the nine FOIA exemptions. Therefore, if a record is not exempt from disclosure, it must be provided to the requester.

(3) Certain records, such as personnel, medical, and similar files, are exempt from disclosure under FOIA Exemption number 6. Under that exemption, disclosure of information pertaining to an individual can be denied only when the disclosure would be “a clearly unwarranted invasion of personal privacy.”

(4) Records or information from investigatory records, including personnel security investigatory records, are exempt from disclosure under the broader standard of “an unwarranted invasion of personal privacy” found in FOIA Exemption number 7. This broader standard applies only to investigatory records.

(5) A disclosure under the FOIA about civilian employees must be in accordance with DCAA Regulation 5410.8¹⁰, but the following information normally may be disclosed from civilian employee records:

(i) Full name.

(ii) Present and past position titles and occupational series.

(iii) Present and past grades.

(iv) Present and past annual salary rates (including performance awards or bonuses, incentive awards, merit pay amount, Meritorious and Distinguished

¹⁰See footnote 1 to § 317.1(a).

Executive Ranks, and allowances and differentials).

(v) Past duty stations.

(vi) Present duty station and future duty station (if finalized), including room numbers, shop designations, or other identifying information regarding buildings or places of employment, unless the duty stations have been determined by the agency to be sensitive, routinely deployable, or located in a foreign territory.

(vii) Position descriptions, identification of job elements, and those performance standards (but not actual performance appraisals) that the disclosure of which would not interfere with law enforcement programs or severely inhibit agency effectiveness.

(6) Disclosure of home addresses and home telephone numbers:

(i) The disclosure under the FOIA of home addresses and telephone numbers normally is considered a clearly unwarranted invasion of personal privacy and is prohibited. However, they may be disclosed if:

(A) The individual has consented, in writing, to the disclosure.

(B) The disclosure is required by the FOIA; or

(C) The disclosure is required by another Federal law, such as 42 U.S.C. 653, which provides assistance to states in locating parents who have defaulted on child support payments.

(ii) When compiling home addresses and telephone numbers, the individual shall be offered the option of authorizing disclosure of the information without further consent for specific purposes, such as locator services. In that case, the information may be disclosed for the stated purpose without further consent. If the information is to be disclosed for any other purpose, a signed consent permitting the additional disclosure must be obtained from the individual.

(iii) Before listing home addresses and home telephone numbers in telephone directories, the individual should be given the opportunity to refuse such a listing. If the individual requests that the home address or telephone number not be listed in the directory, additional fees should not be assessed associated with maintaining

an unlisted number for government-owned telephone services.

(iv) The sale or rental of lists of names and addresses is prohibited unless such action is specifically authorized by Federal law, but this does not prohibit the disclosure of names and addresses otherwise permitted to be made public, such as by DCAA Regulation 5410.10 (32 CFR part 290).

(c) *Disclosures for established routine uses.* (1) Records may be disclosed outside the agency if the disclosure is for an established routine use.

(2) A routine use shall:

(i) Be compatible with and related to the purpose for which the record was created.

(ii) Identify the persons or organizations to whom the record may be disclosed.

(iii) Identify specifically the uses for which the information may be employed by the receiving person or organization; and

(iv) Be contained in the system of records notice published previously in the FEDERAL REGISTER.

(3) A routine use shall be established for each user of the information outside the agency who needs the information for an official purpose.

(4) Routine uses may be established, discontinued, or amended without the consent of the individuals to whom the records pertain. However, new and amended routine uses must be published in the FEDERAL REGISTER at least 30 days before the information may be disclosed under their provisions.

(5) In addition to the routine uses established by the system notices published in the FEDERAL REGISTER, certain common "blanket routine uses" have been established for all systems of records maintained by the agency. These blanket routine uses are published in the FEDERAL REGISTER at the beginning of the listing of system notices for the agency. Unless a system notice specifically excludes a system of records from a blanket routine use, all blanket routine uses apply to that system. See appendix A to this part.

(6) If the "routine user" recipient has not been identified in the FEDERAL REGISTER or if the recipient, though

identified, intends to employ the information for a purpose not published in the FEDERAL REGISTER, the written consent of the individual is required before the disclosure can be made.

(d) *Disclosures to the Bureau of the Census.* Records may be disclosed to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activities under the provisions of 13 U.S.C. 8.

(e) *Disclosures for statistical research or reporting.* Records may be disclosed to a recipient for statistical research or reporting if:

(1) Prior to the disclosure, the recipient has provided adequate written assurance that the records shall be used solely for statistical research or reporting; and

(2) The records are transferred in a form that does not identify individuals.

(f) *Disclosures to the National Archives and Records Administration.* (1) Records may be disclosed to the National Archives and Records Administration for evaluation to determine whether the records have sufficient historical or other value to warrant preservation by the Federal government. If preservation is warranted, the records will be retained by the National Archives and Records Administration, which becomes the official owner of the records.

(2) Records may be disclosed to the National Archives and Records Administration to carry out records management inspections required by Federal law. Such disclosures are authorized by the National Archives and Records Act of 1984, Pub. L. 98-497.

(3) Records transferred to a Federal Records Center operated by the National Archives and Records Administration for storage are not within this category. Those records continue to be maintained and controlled by the agency. The Federal Records Center is considered the custodian agent of the agency.

(g) *Disclosures when requested for law enforcement purposes.* (1) A record may be disclosed to another agency or an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if:

(i) The civil or criminal law enforcement activity is authorized by law (Federal, State, or local); and

(ii) The head of the agency or instrumentality (or his or her designee) has made a written request to DCAA specifying the particular record or portion desired and the law enforcement activity for which it is sought.

(2) Blanket requests for any and all records pertaining to an individual shall not be honored. The requesting agency or instrumentality must specify each record or portion desired and how each relates to the authorized law enforcement activity.

(3) This disclosure provision applies when the law enforcement agency or instrumentality requests the record. If DCAA discloses a record outside the Department of Defense for law enforcement purposes without the individual's consent and without an adequate written request, the disclosure must be pursuant to an established routine use, such as the blanket routine use for law enforcement.

(h) *Disclosures to protect the health or safety of an individual.* (1) Records may be disclosed by any means and to any person pursuant to a showing of compelling circumstances affecting the health or safety of an individual. The affected individual need not be the subject of the record.

(2) Notification of the disclosure (date and what, why, and to whom disclosed) must be sent to the subject of the record. Sending the notification to the last known address is sufficient.

(i) *Disclosures to Congress.* (1) A record may be disclosed to either House of Congress on the initiative of the agency or at the request of either the Senate or House of Representatives as a whole.

(2) A record also may be disclosed to any committee, subcommittee, or joint committee of Congress if the disclosure pertains to a matter within the legislative or investigative jurisdiction of the committee, subcommittee, or joint committee.

(3) Individual members of Congress not acting on behalf of the entire house, a committee, subcommittee, or joint committee have no greater right to have records disclosed to them than any other individual. However, for

Members of Congress making inquiries on behalf of individuals who are subjects of records, a blanket routine use has been established to permit disclosures to individual members of Congress.

(i) When responding to a congressional inquiry made on behalf of a constituent by whose identifier the record is retrieved, there is no need to verify that the individual has authorized the disclosure to the Member of Congress.

(ii) The oral statement of a congressional staff member is sufficient to establish that a request has been received from the individual to whom the record pertains.

(iii) If the constituent inquiry is made on behalf of an individual other than the subject of the record, provide the Member of Congress only that information releasable under the FOIA. The Member of Congress should be advised that the written consent of the subject of record is required before additional information may be disclosed. The subject of record should not be contacted to obtain consent for the disclosure to the Member of Congress unless the congressional office specifically requests that it be done.

(j) *Disclosures to the Comptroller General for the General Accounting Office.* Records may be disclosed to the Comptroller General, or his or her authorized representative, for the performance of the duties of the General Accounting Office.

(k) *Disclosures pursuant to court orders.* (1) Records may be disclosed pursuant to the order of a court of competent jurisdiction.

(2) The court order must bear the signature of a Federal, State, or local judge. Orders signed by court clerks or attorneys are not deemed to be orders of a court of competent jurisdiction. A photocopy of the order, regular on its face, will be sufficient evidence of the court's exercise of its authority if the minimal requirements of DCAA Regulation 5410.11, "Release of Official Information in Litigation and Testimony by DCAA Personnel as Witness."

(3) When a record is disclosed under this provision and the compulsory legal process becomes a matter of public record, make reasonable efforts to notify the subject of the record. Notifica-

tion sent to the last known address of the individual is sufficient.

(l) *Disclosures to consumer reporting agencies.* (1) Certain information may be disclosed to consumer reporting agencies as defined by 31 U.S.C. 952d.

(2) Under these provisions, the following information may be disclosed to a consumer reporting agency:

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

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

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

(3) 31 U.S.C. 952d specifically requires that the FEDERAL REGISTER notice for the system of records from which the information will be disclosed indicate that the information may be disclosed to a consumer reporting agency.

§ 317.62 Disclosures to commercial enterprises.

(a) *General policy.* (1) Records may be disclosed to commercial enterprises only under the criteria established by the FOIA.

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

(3) The policy on personal indebtedness for civilian employees, is contained in DCAA Manual 1400.1, DCAA Personnel Management Manual.

(b) *Disclosure of information.* (1) Any information required to be disclosed by the FOIA may be disclosed to a requesting commercial enterprise.

(2) Commercial enterprises may present a concise statement signed by the individual indicating specific conditions for disclosing information from a record. Statements such as the following, if signed by the individual, are considered sufficient to authorize the disclosure:

I hereby authorize the Defense Contract Audit Agency to verify my Social Security Number or other identifying information and to disclose my home address and telephone number to authorized representatives of (name of commercial enterprise) to be used in connection with my commercial dealings

§ 317.63

with that enterprise. All information furnished will be used in connection with my financial relationship with (name of commercial enterprise).

(3) When a consent statement as described in the preceding paragraph is presented, the information should be provided to the commercial enterprise, unless the disclosure is prohibited by another regulation or Federal law.

(4) Requests should not be honored from commercial enterprises for official evaluations or personal characteristics such as personal financial habits.

§ 317.63 Disclosing health care records to the public.

This section applies to the disclosure of information to the news media and the public concerning individuals treated or hospitalized in DoD medical facilities and, when the cost of care is paid by the agency, in non-Federal facilities.

(a) *Disclosures without the individual's consent.* Normally, the following information may be disclosed without the individual's consent:

(1) Information required to be released by the FOIA, as well as the information listed for military personnel and for civilian employees; and

(2) The following general information concerning medical condition:

(i) Date of admission or disposition; and

(ii) Present medical assessment of the individual's condition in the following terms, if the medical practitioner has volunteered the information:

(A) The individual's condition presently is (stable) (good) (fair) (serious) (critical), and

(B) The patient is conscious, semiconscious, or unconscious.

(b) *Disclosures with the individual's consent.* With the individual's informed consent, any information about the individual may be disclosed. If the individual is a minor or has been declared incompetent by a court of competent jurisdiction, the parent or the appointed legal guardian may give consent on behalf of the individual.

(c) *Disclosures to other government agencies.* This section does not limit otherwise lawful disclosures to other

32 CFR Ch. I (7-1-99 Edition)

government agencies for use in determining eligibility for special assistance or other benefits provided there is a published routine use permitting the disclosure.

§ 317.64 Accounting for disclosures.

(a) *When to keep disclosure accountings.* An accurate record of all disclosures made from a record (including those made with the consent of the individual) should be kept except those made:

(1) To DCAA personnel for use in performing their official duties; and

(2) Pursuant to DCAA Regulation 5410.10 (32 CFR part 290).

(b) *Content of disclosure accountings.* Disclosure accountings shall contain:

(1) The date of the disclosure.

(2) A description of the information disclosed.

(3) The purpose of the disclosure; and

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

(c) *Using disclosure accountings.* When an individual's request to amend the record is granted and when an individual files a statement of disagreement, all persons and agencies listed in the disclosure accounting, except those known to be no longer retaining the record, must be informed.

(d) *Individual access to disclosure accountings.* The record subject has the right of access to the disclosure accounting except when:

(1) The disclosure was made at the request of a civil or criminal law enforcement agency, or

(2) The system of records has been exempted from the requirement to provide access to the disclosure accounting.

(e) *Methods of disclosure accounting.* (1) The agency may use any method of disclosure accounting that will readily provide the necessary disclosure information required.

(2) When numerous similar records are disclosed (e.g., sending payroll checks to banks), identify the category of records disclosed and include the information in some form that can be used to construct a disclosure accounting.

(f) *Retaining disclosure accountings.* The disclosure accounting shall be retained for five years after the disclosure was made or the life of the record, whichever is longer.

Subpart G—Publication Requirements

§ 317.70 Federal Register publication.

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

(i) DCAA Privacy Program procedural rules (32 CFR part 317).

(ii) DCAA exemption rules (32 CFR part 317), and

(iii) Record system notices.

(2) DoD 5025.1-M, “DoD Directives System Procedures,” and DoD Directive 5400.9, “Publication of Proposed and Adopted Regulations Affecting the Public” (32 CFR part 336), contain information on preparing documents for publication in the FEDERAL REGISTER.

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

(c) *Formal rulemaking and notices.* (1) DCAA Privacy Program procedural and exemption rules are subject to the rulemaking procedures prescribed by 32 CFR part 336. These are incorporated automatically into the Code of Federal Regulations.

(2) Record system notices are published in the FEDERAL REGISTER as “notices.” They are not subject to the rulemaking procedures or automatic incorporation into the Code of Federal Regulations.

(d) *Submitting Privacy Program procedural rules for publication.* (1) Procedural rules must be published in the FEDERAL REGISTER first as proposed rules to allow for public comment, then as final rules.

(2) The DCAA Privacy Advisor will submit to the Defense Privacy Office all proposed rules implementing this rule. The submission must conform to the FEDERAL REGISTER format.

(3) This part published as a final rule in the FEDERAL REGISTER shall be in-

corporated by regions as their own rules by reference rather than by republication. A region that simply implements this part as its own rule need not publish it as a final rule in the FEDERAL REGISTER.

(4) Amendments to agency rules are submitted in the same manner as the original rules.

(5) The Defense Privacy Office, DA&M, reviews and submits all DoD component rules, and amendments to rules to the FEDERAL REGISTER for publication.

(e) *Submitting exemption rules for publication.* (1) Exemption rules must be published in the FEDERAL REGISTER first as proposed rules to allow for public comment, then as final rules.

(2) No system of records shall be exempt from any provision of the Privacy Act until the exemption rule has been published in the FEDERAL REGISTER as a final rule.

(3) Proposed exemption rules should be submitted in proper format through the agency Privacy Advisor to the Defense Privacy Office, DA&M, for review and submittal to the FEDERAL REGISTER for publication.

(4) Amendments to exemption rules are submitted in the same manner as the original exemption rules.

(f) *Submitting record system notices for publication.* (1) Although system notices are not subject to formal rulemaking procedures, advance public notice must be given before the agency may begin to collect information for or maintain a new system of records. The notice procedures require that:

(i) The record system notice describe the contents of the record system and the purposes and routine uses for which the information will be used and disclosed.

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

(iii) The notice contain the date the system of records will become effective.

(2) System notices shall be submitted through the agency Privacy Advisor to the Defense Privacy Office, DA&M, for publication in the FEDERAL REGISTER.

§ 317.71

32 CFR Ch. I (7-1-99 Edition)

§ 317.71 Exemption rules.

(a) *General procedures.* This section provides guidance for establishing exemptions for systems of records.

(b) *Content of exemption rules.* (1) Each proposed exemption rule submitted for publication in the FEDERAL REGISTER must contain:

(i) The agency identification and name of the record system for which an exemption will be established.

(ii) The subsection(s) of the Privacy Act which grants the agency authority to claim an exemption for the system (e.g., subsection (k)(2) or (k)(5) of the Privacy Act).

(iii) The particular subsection(s) of the Privacy Act which the system will be exempt from (e.g., subsections (c)(3), (d)(1)-(5) of the Privacy Act); and

(iv) The reasons why an exemption from the particular subsection identified in the preceding subparagraph is being claimed.

§ 317.72 System of records notices.

(a) *Contents of a record system notice.* The following data captions are prescribed by the Office of the FEDERAL REGISTER and must be included for each system notice:

(1) System identifier.

(2) System name.

(3) System location.

(4) Categories of individuals covered by the system.

(5) Categories of records in the system.

(6) Authority for maintenance of the system.

(7) Purpose(s).

(8) Routine uses of records maintained in the system, including categories of users and purposes of the uses.

(9) Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system.

(10) System manager(s) and address.

(11) Notification procedures.

(12) Record access procedures.

(13) Contesting records procedures.

(14) Record source categories; and

(15) Exemptions claimed for the system.

(b) *System identification.* The system identifier must appear in all system notices. It is limited to 21 positions, in-

cluding agency code, file number, symbols, punctuation, and spaces.

(c) *System name.* (1) The system name must indicate the general nature of the system of records and, if possible, the general category of individuals to whom it pertains.

(2) Acronyms should be established parenthetically following the first use of the name (e.g., "Field Audit Office Management Information System (FMIS)"). Acronyms shall not be used unless preceded by such an explanation.

(3) The system name may not exceed 55 character positions, including punctuation and spaces.

(d) *System location.* (1) For a system maintained in a single location, provide the exact office name, organizational identity, routing symbol, and full mailing address. Do not use acronyms in the location address.

(2) For a geographically or organizationally decentralized system, describe each level of organization or element that maintains a portion of the system of records.

(3) For an automated data system with a central computer facility and input or output terminals at geographically separate locations, list each location by category.

(4) If multiple locations are identified by type of organization, the system location may indicate that official mailing addresses are published as an appendix to the agency's compilation of systems of records notices in the FEDERAL REGISTER. If no address directory is used, or if the addresses in the directory are incomplete, the address of each location where a portion of the record system is maintained must appear under the "system location" caption.

(5) Classified addresses shall not be listed, but the fact that they are classified shall be indicated.

(6) The U.S. Postal Service two-letter state abbreviation and the nine-digit zip code shall be used for all domestic addresses.

(e) *Categories of individuals covered by the system.* (1) Clear, nontechnical terms shall state the specific categories of individuals to whom records in the system pertain.

(2) Broad descriptions such as “all DCAA personnel” or “all employees,” should be avoided unless the term actually reflects the category of individuals involved.

(f) *Categories of records in the system.*

(1) Clear, nontechnical terms shall be used to describe the types of records maintained in the system.

(2) The description of documents should be limited to those actually retained in the system of records. Source documents should not be described that are used only to collect data and then are destroyed.

(g) *Authority for maintenance of the system.* (1) The system of records must be authorized by a Federal law or Executive Order of the President, and the specific provision must be cited.

(2) When citing federal laws, include the popular names (e.g., “5 U.S.C. 552a, The Privacy Act of 1974”) and for Executive Orders, the official titles (e.g., “Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons”).

(3) The Directive establishing the agency, DoD Directive 5105.36 (32 CFR part 357), as well as the law that authorizes the Secretary of Defense to issue Directives, 10 U.S.C. 133 should be cited.

(h) *Purpose(s).* The specific purpose(s) for which the system of records was created and maintained; that is, the uses of the records within the agency and the rest of the Department of Defense should be listed.

(i) *Routine uses.* (1) All disclosures of the records outside the agency, including the recipient of the disclosed information and the uses the recipient will make of it should be listed.

(2) If possible, the specific activity or element to which the record may be disclosed (e.g., “to the Department of Veterans Affairs, Office of Disability Benefits”) should be listed.

(3) General statements such as “to other Federal Agencies as required” or “to any other appropriate Federal agency” should not be used.

(4) The blanket routine uses, published at the beginning of the agency’s compilation, applies to all system notices, unless the individual system notice states otherwise.

(j) *Policies and practices for storing, retrieving, accessing, retaining, and disposing of records.* This section is divided into four parts.

(1) *Storage:* The method(s) used to store the information in the system (e.g., “automated, maintained in computers and computer output products” or “manual, maintained in paper files” or “hybrid, maintained in paper files and in computers”) should be stated. Storage does not refer to the container or facility in which the records are kept.

(2) *Retrievability:* How records are retrieved from the system (e.g., “by name,” “by SSN,” or “by name and SSN”) should be indicated.

(3) *Safeguards:* The categories of agency personnel who use the records and those responsible for protecting the records from unauthorized access should be stated. Generally the methods used to protect the records, such as safes, vaults, locked cabinets or rooms, guards, visitor registers, personnel screening, or computer “fail-safe” systems software should be identified. Safeguards should not be described in such detail as to compromise system security.

(4) *Retention and disposal:* Describe long records are maintained. When appropriate, the length of time records are maintained by the agency in an active status, when they are transferred to a Federal Records Center, how long they are kept at the Federal Records Center, and when they are transferred to the National Archives or destroyed should be stated. If records eventually are destroyed, the method of destruction (e.g., shredding, burning, pulping, etc), should be stated. If the agency rule is cited, the applicable disposition schedule shall also be identified.

(k) *System manager(s) and address.* (1) The title (not the name) and address of the official or officials responsible for managing the system of records should be listed.

(2) If the title of the specific official is unknown, such as with a local system, the local director or office head as the system manager should be indicated.

§ 317.73

32 CFR Ch. I (7-1-99 Edition)

(3) For geographically separated or organizationally decentralized activities with which individuals may correspond directly when exercising their rights, the position or title of each category of officials responsible for the system or portion thereof should be listed.

(4) Addresses that already are listed in the agency address directory; or simply refer to the directory should not be included.

(1) *Notification procedures.* (1) Notification procedures describe how an individual can determine if a record in the system pertains to him or her.

(2) If the record system has been exempted from the notification requirements of subsection (f)(1) or subsection (e)(4)(G) of the Privacy Act, it should be so stated.

(3) If the system has not been exempted, the notice must provide sufficient information to enable an individual to request notification of whether a record in the system pertains to him or her. Merely referring to the agency's procedural rules is not sufficient.

(4) This section should also include:

(i) The title (not the name) and address of the official (usually the system manager) to whom the request must be directed;

(ii) Any specific information the individual must provide in order for the agency to respond to the request (e.g., name, SSN, date of birth, etc.); and

(iii) Any description of proof of identity for verification purposes required for personal visits by the requester.

(m) *Record access procedures.* (1) This section describes how an individual can review the record and obtain a copy of it.

(2) If the system has been exempted from access and publishing access procedures under subsections (d)(1) and (e)(4)(H), respectively, of the Privacy Act, it should be so indicated.

(3) If the system has not been exempted, describe the procedures an individual must follow in order to review the record and obtain a copy of it, including any requirements for identity verification.

(4) If appropriate, the individual may be referred to the system manager or another agency official who shall pro-

vide a detailed description of the access procedures. Any addresses already listed in the address directory should not be repeated.

(n) *Contesting record procedures.* (1) This section describes how an individual may challenge the denial of access or the contents of a record that pertains to him or her.

(2) If the record system has been exempted from allowing amendments to records or publishing amendment procedures under subsections (d)(2) and (e)(4)(H), respectively, of the Privacy Act, it should be so stated.

(3) If the system has not been exempted, the procedures an individual must follow should be described in order to challenge the content of a record pertaining to him or her, or explain how he or she can obtain a copy of the procedures (e.g., by contacting the system manager or another agency official).

(o) *Record source categories.* (1) If the system has been exempted from publishing record source categories under subsection (e)(4)(I) of the Privacy Act, it should be so stated.

(2) If the system has not been exempted, this caption must describe where the agency obtained the information maintained in the system.

(3) Describing the record sources in general terms is sufficient; specific individuals, organizations, or institutions need not be identified.

(p) *Exemptions claimed for the system.*

(1) If no exemption has been established for the system, indicate "None."

(2) If an exemption has been established, state under which provision of the Privacy Act it is established (e.g., "Parts of this system of records may be exempt under 5 U.S.C. 552a(k)(2)").

§ 317.73 New and altered record systems.

(a) *Criteria for a new record system.* (1) A new system of records is one for which no existing system notice has been published in the FEDERAL REGISTER.

(2) If a notice for a system of records has been canceled or deleted and the agency desires to reinstate or reuse the system, a new system notice must be published in the FEDERAL REGISTER.

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

(1) A significant increase or change in the number or types of individuals about whom records are maintained requires a change to the "categories of individuals covered by the system" caption in the system notice and might require changes to the "purpose(s)" caption.

(i) For example, a decision to expand a system of records that originally covered personnel assigned to only one location to cover personnel at several locations would constitute an altered system.

(ii) An increase in the number of individuals covered due to normal growth is not an alteration.

(iii) A decrease in the number of individuals covered is not an alteration, but it is an amendment.

(2) A change that expands the types or categories of information maintained requires a change in the "categories of records in the system" caption in the system notice.

(i) For example, a personnel file that has been expanded to include medical records would be an alteration.

(ii) Adding to a personnel file a new data element that is clearly within the scope of the categories of records described in the existing notice is not an alteration, but is an amendment.

(3) A change that alters the purpose for which the information is used requires changing the "purpose(s)" caption in the system notice. In order to be an alteration, the change must be one that is not reasonably inferred from any of the existing purposes.

(4) A change to equipment configuration (either hardware or software) that creates substantially greater use of records in the system requires changing the "storage" caption in the system notice. For example, placing interactive computer terminals at regional offices to use a system formerly used only at the Headquarters would be an alteration.

(5) A change in the manner in which records are organized or in the method by which records are retrieved requires changing the "Retrievability" caption in the system notice.

(i) Combining record systems due to a reorganization within the agency would be an alteration.

(ii) Retrieving by SSNs records that previously were retrieved only by names would be an alteration if the present notice failed to indicate retrieval by SSNs.

(c) *Reports of new and altered systems of records.* (1) Under subsection (o) of the Privacy Act, reports of new and altered systems of records must be submitted to Congress and the Office of Management and Budget.

(2) The agency shall submit reports of new or altered systems to the Defense Privacy Office, DA&M, before collecting information for new systems or altering an existing system.

(3) The Defense Privacy Office, DA&M, shall coordinate all reports of new or altered systems with the Office of the Assistant Secretary of Defense (Legislative Affairs) and the Office of the General Counsel, Department of Defense.

(4) The Defense Privacy Office, DA&M, shall prepare, for the approval and signature of the Director, Administration and Management, Office of the Secretary of Defense, transmittal letters to Congress and the Office of Management and Budget.

(d) *Time limits before implementing routine uses.* After publishing a system notice in the FEDERAL REGISTER, 30 days must elapse before routine uses may be employed.

§ 317.74 Amendment and deletion of system notices.

(a) *Criteria for an amended record system.* Minor changes to published system notices are considered amendments rather than alterations. Amendments must also be published in the FEDERAL REGISTER, but a new or altered system report does not have to be accomplished.

(b) *Amending a system notice.* In submitting an amendment to a system notice for publication in the FEDERAL REGISTER, the agency must include:

(1) The system identification and name.

(2) A description of the specific changes proposed; and

§ 317.80

32 CFR Ch. I (7–1–99 Edition)

(3) The full text of the system notice as amended.

(c) *Deleting a system notice.* (1) When a system of records is discontinued, incorporated into another system, or determined to be no longer subject to this rule, a deletion notice must be published in the FEDERAL REGISTER.

(2) The deletion notice shall include:

(i) The system identification number and name.

(ii) The FEDERAL REGISTER citation of the latest publication of the system.

(iii) The reason for the deletion.

(3) If a system is deleted through combination or merger with another system, identify the successor system in the deletion notice.

(d) *Submitting amendments and deletions for publication.* (1) Amendments and deletions should be submitted through the agency Privacy Advisor to the Defense Privacy Office, DA&M, which will transmit them to the FEDERAL REGISTER for publication.

(2) At least one original in proper format should be included in the submission.

(3) Multiple amendments and deletions, and combinations of amendments and deletions, may be submitted together.

Subpart H—Training Requirements

§ 317.80 Statutory training requirements.

(a) *Establishing rules of conduct.* Under subsection (e)(9) of the Privacy Act, the agency is required to establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record.

(b) *Training.* The agency shall train all personnel involved in the functions described in the preceding paragraph. The training shall include instruction in the rules of conduct and all requirements prescribed by the Privacy Act, including the penalties for noncompliance.

§ 317.81 DCAA training programs.

(a) *Personnel to be trained.* (1) To conform with Office of Management and Budget guidance, compliance with the

statutory training requirements requires informed and active support of all agency personnel. All personnel who in any way use or operate systems of records, or who are engaged in the development of procedures for handling records, must be taught the requirements of the Privacy Act and must be trained in the agency's procedures for the implementation of the Privacy Act.

(2) Personnel to be trained include, but are not limited to, those engaged in the following:

(i) Personnel management.

(ii) Personnel finance.

(iii) Medical care.

(iv) Investigations of personnel.

(v) Records management (reports, forms, records, and related functions).

(vi) Computer systems development and operation.

(vii) Communications.

(viii) Statistical data collection and analysis, and

(ix) Performing other functions subject to this rule.

(b) *Types of training.* The agency shall establish the following three levels of training for those persons who are involved with the design, development, operation, or maintenance of any system of records. The training shall be provided to persons before or shortly after assuming the duties associated with the level of involvement.

(1) *Orientation training.* Orientation training that provides a general understanding of the individual's rights under the Privacy Act.

(2) *Specialized training.* Training concerning the application of this part to specialized areas of job performance.

(3) *Management training.* Training concentrated on factors affecting decisions made by managers under the Privacy Program, such as system managers, denial authorities, and managers of the specific functions listed.

(c) *Methods of training.* The agency is responsible for developing training methods that will meet this criteria. Such methods may include formal and informal (on-the-job) programs, if those personnel giving the training have, themselves, been trained.

Subpart I—Computer Matching Program Procedures

§ 317.90 General.

(a) *Scope.* The Privacy Act and this rule are applicable to certain types of computer matching--the computer comparison of automated systems of records.

(b) *Compliance.* Although the Privacy Act provides for specific procedures, the Act is not in itself authority for carrying out any matching activity. Compliance with this chapter does not relieve the agency of the obligation to comply with any other requirements of the Privacy Act and this part.

(c) *Matching programs covered by the Privacy Act.* There are two specific kinds of matching programs that are fully governed by the Privacy Act and this part. These are:

(1) Matches using records from Federal personnel or payroll systems of records. See also definitions of this part.

(2) Matches involving Federal benefit programs to accomplish one or more of the following purposes:

(i) To determine eligibility for a Federal benefit.

(ii) To comply with benefit program requirements.

(iii) To effect recovery of improper payments or delinquent debts from current or former beneficiaries.

(d) *Automated comparisons.* The record comparison must be a computerized comparison, manual comparisons are not covered, involving records from:

(1) Two or more automated systems of records (i.e., systems of records maintained by Federal agencies that are subject to the Privacy Act); or,

(2) An agency's automated system of records and automated records maintained by a non-Federal agency (i.e., state or local government or agent thereof).

(e) *Features of a matching program.* A covered computer matching program entails not only the actual computerized comparison, but also preparing and executing a written agreement between the participants, securing approval of the Defense Data Integrity Board, publishing a matching notice in the FEDERAL REGISTER before the

match begins, ensuring that investigation and due process are completed, and taking ultimate action, if any.

§ 317.91 Federal personnel or payroll record matches.

(a) *Scope.* These computer matching programs include matches comparing records from agency automated Federal personnel or payroll systems of records with such automated like records of another Federal agency; or with a non-Federal agency. It also includes matches between DoD components or within the agency itself (internal matches).

(b) *Computerized comparisons.* The matching must be done using a computer. Manual comparisons are not covered.

(c) *Exclusion.* Matches must be done for other than "routine administrative purposes."

(d) *Internal matches.* In some instances, a covered match may take place within the agency or with another DoD component. For example, the agency may wish to determine whether any of its own personnel, participating in a benefit program administered by the Department of Defense, are not complying with the program's eligibility requirements. This internal match will certainly result in an adverse action if ineligibility is discovered. Therefore, it is covered by the requirements of the Privacy Act. The agency should not attempt to avoid the reach of the Act, for example, by improperly combining dissimilar systems into a single system, matching data within that system to make an eligibility determination, and arguing that the match is not covered because only one system of records is involved.

(e) *Categories of record subjects.* The categories of individuals whose records are used in this type of matching program must be carefully analyzed before making a determination whether a proposed match is covered. All information on subjects of record is maintained in the agency's system of records, but matching under the particular programs covered by this subsection is limited to "Federal personnel." For matching purposes, a Federal personnel system of records should

§ 317.92

not be confused with, or limited to, the commonly recognized personnel system of records maintained by a civilian personnel office or a military assignment branch. The agency may be maintaining within a single system of records several categories of records relating to Federal personnel and other categories on non-Federal personnel, e.g., contractor personnel, applicants, dependents, etc. Some categories may be covered while others may not. Unlike "Federal personnel," the subjects of record of payroll record systems are easily discerned.

(f) *Matching purpose.* The purpose of a Federal personnel or payroll records match must be to take some adverse action, financial, personnel, disciplinary, or other adverse action against Federal personnel.

§ 317.92 Federal benefit matches.

(a) *Categories of subjects covered.* The Privacy Act provisions cover only the following categories of subjects of record for Federal benefit matches.

(1) Applicants for Federal benefit programs (i.e., individuals initially applying for benefits).

(2) Program beneficiaries (i.e., individuals currently receiving or formerly receiving benefits).

(3) Providers of services to support such programs (i.e., those deriving income from them such as health care providers).

(b) *Types of programs covered.* Only Federal benefit programs providing cash or in-kind assistance to individuals are covered by the Privacy Act. State programs are not covered. Programs using records about subjects who are not "individuals". See definitions of this part (§ 317.3).

(c) *Matching purpose.* A Federal benefit match must have as its purpose one or more of the following:

(1) Establishing or verifying initial or continuing eligibility for Federal benefit programs.

(2) Verifying compliance with the requirements, either statutory or regulatory, of such programs.

(3) Recouping payments or delinquent debts under such Federal benefit programs.

32 CFR Ch. I (7-1-99 Edition)

(d) *Summary of basic requirements.* Four basic elements:

(1) Computerized comparison.

(2) Categories of subjects.

(3) Federal benefit program, and

(4) Matching purpose, must all be present before a matching program is covered under the Privacy Act.

§ 317.93 Matching program exclusions.

The following are not included under the definition of a matching program. The agency is not required to comply with the computer matching provisions of the Privacy Act, although it may be required to comply with any other applicable provisions of the Act and this part.

(a) *Statistical matches whose purpose is solely to produce aggregate data stripped of personal identifiers.* This does not mean that the data bases used in the match must be stripped prior to the match, but only that the results of the match must not contain data identifying any individual. Implicit in this exception is that this kind of match is not done to take action against specific individuals.

(b) *Statistical matches whose purpose is in support of any research or statistical project.* The results of these matches need not be stripped of identifiers, but they must not be used to make decisions that affect the rights, benefits or privileges of specific individuals.

(c) *Pilot matches.* This exclusion covers small scale sampling matches whose purpose is to gather cost-benefit data on which to premise a decision about engaging in a full-fledged matching program. Pilot matches must be retained in a statistical information gathering channel. It is at this point that the component can decide whether to conduct a statistical data gathering match without consequences to the subjects of record or a full-fledged program where results will be used to take specific action against them. To avoid possible misuse of pilot matches and to ensure full compliance with the Privacy Act, these matches must be approved by the Defense Data Integrity Board.

(d) *Law enforcement investigative matches whose purpose is to gather evidence against a named person or persons*

in an existing investigation. (1) To be eligible for the exclusion the match must be performed by an activity of a component whose principal function involves enforcement of criminal laws, i.e., an activity that is authorized to exempt certain of its systems of records under subsection (j)(2) of the Privacy Act.

(2) The match must flow from an investigation already underway which focuses on a named person or persons. Subjects identified generically, e.g., "program beneficiaries," are not eligible.

(3) The investigation may be into either criminal or civil law violations.

(4) In the context of this exclusion only, person or persons could include subjects that are other than individuals as defined in the Privacy Act, such as corporations or other business entities. For example, a business entity could be named subject of the investigation and records matched could be those of customers or clients.

(5) The match must be for the purpose of gathering evidence against the named person or persons.

(e) *Tax administration matches.* (1) Matches involving disclosures of taxpayer return information to state or local tax officials pursuant to section 6103(d) of the Internal Revenue Code.

(2) Tax refund offset matches accomplished pursuant to the Deficit Reduction Act of 1984.

(3) Matches done for tax administration pursuant to section 6103(b)(4) of the Internal Revenue Code.

(4) Tax refund offset matches conducted pursuant to other statutes provided approval of the Office of Management and Budget is obtained.

(f) *Routine administrative matches using Federal personnel records.* These are matches between the agency and other Federal agencies or between the agency and non-Federal agencies for administrative purposes that use data bases that contain records predominantly relating to Federal personnel. The term "predominantly" means that the percentage of records in the system that are about Federal employees must be greater than of any other category contained therein. For the purpose of disclosing records subject to the Pri-

vacancy Act, the Department of Defense is considered a single agency.

(1) The purpose of the match must not be intended to result in an adverse action. Matches whose purpose is to take any adverse financial, personnel, disciplinary or other adverse action against Federal personnel whose records are involved in the match, are not excluded from the Act's coverage.

(2) An example of a match that is excluded is an agency's disclosure of time and attendance information on all agency employees to the Department of the Treasury in order to prepare the agency's payroll.

(3) This exclusion does not bring under the Act's coverage matches that may ultimately result in an adverse action. It only requires that their purpose not be intended to result in an adverse action.

(g) *Internal matches using only records from DoD systems of records.* (1) Internal matches (conducted within the Department of Defense) are excluded on the same basis as Federal personnel record matching provided no adverse intent as to a Federal employee motivates the match.

(2) This exclusionary provision does not disturb subsection (b)(1) of the Act permitting disclosure to DoD employees on an official need-to-know basis.

(3) The purpose of the internal match must not be to take any adverse financial, personnel, disciplinary, or other adverse action against Federal personnel.

(h) *Background investigation and foreign counterintelligence matches.* Matches done in the course of performing a background check for security clearances of Federal personnel or Federal contractor personnel are not covered. Matches done for the purpose of foreign counterintelligence are also not covered.

§317.94 Conducting matching programs.

(a) *Source and recipient agencies.* The agency, if undertaking a matching program, should consider if it will be a "source agency" or a "recipient agency" for the match and be prepared to meet the following requirements:

(1) The recipient agency does the matching. It receives the data from

system of records of other Federal agencies or data from state and local governments and actually performs the match by computer.

(2) The recipient agency is responsible for publishing a notice in the FEDERAL REGISTER of the matching program. Where a state or local agency is the recipient, the Federal source agency is responsible for publishing the notice.

(3) A Federal source agency discloses the data from a system of records for the match. A non-Federal agency may also be a source, but the record data will not be from a system of records. The "system of records" concept under the Privacy Act does not apply to the recordkeeping practices of state or local governmental agencies.

(4) The recipient Federal agency, or the Federal source agency in a match performed by a non-Federal agency, is responsible for reporting the match. This agency must contact the other participants to gather the information necessary to make a unified report as required by § 317.100.

(5) In some circumstances, a source agency may be the instigator and ultimate beneficiary of the matching program, as when an agency lacking computer resources uses another agency to perform the match; or when as a practical matter, an agency may not wish to release and disclose its data base to another agency as a source because of privacy safeguard considerations.

(b) *Compliance with the system of records and disclosure provisions.* (1) The agency must ensure that it identifies the system(s) of records involved in the matching program and has published the necessary notice(s) in the FEDERAL REGISTER.

(2) The Privacy Act does not itself authorize disclosures from system of records for the purpose of conducting a matching program. The agency must justify any disclosures outside the Department of Defense under subsection (b) of the Act. This means obtaining the written consent of the subjects of record for the disclosure or relying on one of the 12 non-consensual disclosures exceptions to the written consent rule. To rely on the routine use exception (b)(3), the agency must have already established the routine use (pub-

lished in the FEDERAL REGISTER), or in the alternative, must comply with subsections (e)(4)(d) and (e)(11) of the Act which means amending the record system notice to add an appropriate routine use for the match. An amendment requires publication in the FEDERAL REGISTER with a 30 day waiting period for public comment.

(3) The routine use permitting disclosure for the match must be compatible with and related to the purpose for which the record was initially compiled.

(4) The routine use for the match in a record system notice shall clearly indicate that it entails a computer matching program with a specific agency for an established purpose and intended objective. For purposes of matching, a routine use must state that a disclosure may be made for a matching program. The agency may not rely on an existing established routine use to meet the requirements of the Act unless it expressly permits disclosure for matching purposes.

(c) *Prior notice to record subjects.* Subjects of record must receive prior notice that their records may be matched. This may be done by direct and/or constructive notice.

(1) Direct notice may be given when there is some form of contact between the government and the subject. Information can be furnished to individuals on the application form when they apply for a benefit, in a notice that arrives with a benefit, or in correspondence they receive in the mail. Use of the advisory Privacy Act Statement is an acceptable manner to provide direct notice to subjects of record at the time of application. The agency shall provide direct notice for front-end eligibility verification matching programs whose purpose is to validate an applicant's initial eligibility for a benefit and later to determine continued eligibility using the Privacy Act Statement on the application form. Providers of services should be given notice (Privacy Act Statement) on the form on which they apply for reimbursement for services provided. Providing notice of matching programs using the Privacy Act Statement shall be part of the normal process of implementing a Federal benefits program. The agency

shall insure records contain appropriate revisions.

(2) Constructive notice can only be given by an appropriate routine use disclosure provision of the affected system of records to be used in the match. For purely internal matching program uses, amend the "Purpose(s)" element of the record system notice to specifically reflect those internal computer matches performed. The constructive notice method requires publication in the FEDERAL REGISTER. Examples of when constructive notice may be used:

(i) For matching programs whose purpose is to locate individuals in order to recoup payments improperly granted to former beneficiaries, direct notice may well be impossible and constructive notice may have to suffice.

(ii) The agency that discloses records to a state or local government in support of a non-Federal matching program is not obligated to provide direct notice to each subject of record. FEDERAL REGISTER publication in this instance is sufficient.

(iii) Investigative matches where direct notice immediately prior to a match would provide the subject an opportunity to alter behavior.

(3) The agency shall also provide periodic notice whenever an application is renewed, or at the least during the period the match is authorized to take place by providing notice accompanying the benefit as approved by the Defense Data Integrity Board.

(d) *Publication of the matching notice.*

(1) The matching agency is required to publish in the FEDERAL REGISTER a notice of any proposed matching program or alteration of an established program at least 30 days prior to conducting the match for any public comment. Only one notice is required. When a non-Federal agency is the matching agency, the source agency shall be responsible for the publication. The proposed matching notice for publication shall be submitted in FEDERAL REGISTER format and included in the agency report. The notice shall contain the customary preamble and contain the required information in sufficient detail describing the match so that the reader will easily understand the nature and purpose of the match, including any adverse consequences.

(2) The preamble to the notice shall be prepared by the Defense Privacy Office, DA&M, and shall contain:

(i) The date the transmittal letters to OMB and Congress are signed.

(ii) A statement that the matching program is subject to review by OMB and Congress and shall not become effective until that review period has elapsed.

(iii) A statement that a copy of the agreement shall be available upon request to the public.

(3) The agency shall provide:

(i) Name of participating agency or agencies.

(ii) Identity of the source agency and the recipient agency, or in the case of an internal DoD matching, the Component(s) involved.

(iii) Purpose of the match being conducted to include a description of the matching program and whether the program is a one-time or a continuing program.

(iv) Legal authority for conducting the matching program. Do not cite the Privacy Act as it provides no independent authority for carrying out any matching activity. If at all possible, use the U.S. Code citations rather than the Public Law as access to the Public Laws is more difficult. Avoid citing housekeeping statutes such as 5 U.S.C. 301, but rather cite the underlying programmatic authority for collecting, maintaining, and using the information even if it results in citing the Code of Federal Regulations or a DoD directive or regulation. Whenever possible, the popular name or subject of the authority should be given, as well as a statute, public law, U.S. Code, or Executive Order number; for example: The Debt Collection Act of 1982 (Pub. L. 97-365) 5 U.S.C. 5514, Installment deduction of indebtedness.

(v) A complete description of the system(s) of records that will be used in the match. Include the system identification, name, and the official FEDERAL REGISTER citation, date published, including any published amendments thereto. Provide a positive statement that the system(s) contains an appropriate routine use provision authorizing the disclosure of the records for the purpose of conducting the computer matching program.

§ 317.95

32 CFR Ch. I (7-1-99 Edition)

(Note: In the case of internal DoD matches, the "purpose(s)" element of the system(s) involved.) If non-Federal records are involved, a complete description to include the specific source, address, and category of records to be used, e.g., Human Resources Administration Medicaid File, City of New York, Human Resources Administration, 250 Church Street, New York, NY 10013.

(vi) A complete description of the category of records and individuals covered from the record system(s) to be used, the specific data elements to be matched, and the approximate number of records that will be matched.

(vii) The projected start and ending dates for a one-time match or the inclusive dates for a continuing match.

(viii) The address for receipt of any public comment or inquiries concerning the notice shall indicate: Director, Defense Privacy Office, 400 Army Navy Drive, Room 205, Arlington, VA 22202-2884.

§ 317.95 Providing due process to matching subjects.

(a) *Independent verification and notice.* Subjects of record of matching programs shall be afforded certain due process procedures when a match uncovers any disqualifying or adverse information about them. No recipient agency, non-Federal agency, or source agency shall take any adverse action against an individual until such agency has independently verified such information and the individual has received a notice from the agency containing a statement of its findings and gives the individual the opportunity to contest the findings before making a final determination. The agency shall not take any adverse action based on the raw results of a computer matching program. Adverse information developed by a match must be investigated and verified prior to any action being taken.

(b) *Waiver of independent verification procedures.* Program officials may request the Data Integrity Board waive the independent verification requirement after they have identified the type of matching data eligible for a waiver and conducted a thorough determination of the data's accuracy.

The only data eligible for waiver is that which identifies the individual and the amount of benefits paid under a federal benefit program. The data must not be ambiguous. After the Data Integrity Board determines that the data qualifies for the waiver procedure, the program official must present convincing evidence to the Data Integrity Board of the recipient agency to permit the Board to assert a high degree of confidence in the accuracy of the data. The following elements are examples of evidence which will assist a Board in making such a determination: A description of the databases involved including how the information is acquired and maintained; the system manager's overall assessment of the reliability of the systems and the accuracy of the data they contain; the results of any assessments or audits conducted; any material or significant weaknesses under various statutes; security controls in place; previous security assessments; any historical data relating to program error rates; and any information relating to the currency of the data. If the Board approves the waiver, it will notify the source agency and the program officials.

(c) *Independent investigation.* Conservation of resources dictates that the procedures for affording due process be flexible and suited to the data being verified and the consequences to the individual of making a mistake. If the source agency has established a high degree of confidence in the quality of its data and it can demonstrate that its quality control processes are rigorous, the recipient agency may choose to expend fewer resources in independently verifying the data. Absolute confirmation is not required. The agency should bring some degree of reasonableness to the process of verifying data. Some methods to consider are:

- (1) The individual subject of record who is the best source where practical, and
- (2) Researching source documents.

(d) *Notice and opportunity to contest.* The agency is required to notify matching subjects of adverse information uncovered during a matching program and give them an opportunity to contest and explain before the agency

makes a final determination. Recipients already receiving benefits may not have them suspended or reduced pending expiration of the contest period. Individuals have 30 days to respond to a notice of adverse action, unless a statute or regulation grants a longer period. The period runs from the date of the notice until 30 calendar days. The agency shall allow an additional five days for mailing time before ending the notice period. If an individual contacts the agency within the notice period (35 days) and indicates his or her acceptance of the validity of the adverse information, the agency may take immediate action to deny or terminate. The agency may also take action if the period expires without a response.

(e) *Combining verification and notice requirements.* It may be appropriate to combine the verification and notice requirements into a single step, especially if the subject of record is the best source for verification. In this manner, the adverse finding and notice of the opportunity to contest are compressed into a single action. This method is dependent upon the confidence, reliability and quality of the data. Careful thought should be given as to when to apply this method. It may be applicable in special cases, but should not be considered as a routine process. To ensure that this consideration takes place, it shall be the responsibility of the Defense Data Integrity Board to make a formal determination as to when it is appropriate to compress the verification and notice into a single period.

(f) *Individual status pending due process.* The agency may not make a final determination as to applicants for Federal benefit programs whose eligibility is being verified through a matching program until they have completed the due process steps the Act requires. This does not require placing an applicant on the rolls pending a determination, but only that the agency not make a final determination. However, if a subject is already receiving benefits, the benefits shall not be suspended or reduced until due process steps have been completed. If the specific Federal benefit program involved in the match has its own due process requirements, those requirements may suffice for the

purposes of the Privacy Act, provided the Defense Data Integrity Board determines that they are at least as strong as the Privacy Act's provisions.

(g) *Exclusion.* (1) If the agency determines a potentially significant effect on public health or safety is likely, it may take appropriate action, notwithstanding these due process requirements.

(2) In such cases, the agency shall include the possibility of suspension of due process for this reason in its matching program agreement.

§ 317.96 Matching program agreement.

(a) *Requirements.* The agency should allow sufficient lead time to ensure that a matching agreement between the participants can be negotiated and signed in time to secure the Defense Data Integrity Board decision before the match begins. The agency, if receiving records from or disclosing records to a non-Federal agency for use in a matching program, is responsible for preparing the matching agreement and should solicit relevant data from the non-Federal agency where necessary. Both Federal source and recipient agencies must have the matching agreement approved by their respective Data Integrity Boards. In cases where matching takes place entirely within the Department of Defense, the agency may satisfy the matching agreement requirements by preparing a Memorandum of Understanding (MOU) between the systems of records managers involved. Before the agency may participate in a matching program the Defense Data Integrity Board must have evaluated the proposed match and approved the terms of the matching agreement or MOU.

(b) *Agreements or MOUs must contain the following elements—*(1) *Purpose and legal authority.* Citation of the Federal or state statutory or regulatory authority for undertaking the matching program. Do not cite the Privacy Act.

(2) *Justification and expected results.* A full explanation of why a computer matching program, as opposed to some other form of activity, is being proposed and what the expected results will be, including a specific estimate of any savings.

(3) *Records description.* A full identification of the system of records (FEDERAL REGISTER citations) or non-Federal records, number of subjects of record, and what data elements will be included in the match.

(4) *Dates.* An indication of whether the match is a one-time or continuing program (not to exceed 18 months) and the projected starting and completion dates for the match.

(5) *Prior notice to subjects of record.* A description of the direct and constructive notice procedures afforded the subjects of record. Copies of the published applicable record system notices involved and all applicable forms containing the appropriate Privacy Act Statement being used by the participants of the proposed match should be provided.

(6) *Verification procedures.* A full description of the methods the agency will use to independently verify the information obtained through the matching program.

(7) *Disposition of matched items.* A statement that the information generated as a result of the matching program will be destroyed as soon as it has served the matching program's purpose and any legal retention requirements the agency establishes in conjunction with the National Archives and Records Administration or other cognizant authority.

(8) *Security procedures.* A description of the administrative, technical and physical safeguards to be used in protecting the information. They should be commensurate with the level of sensitivity of the data.

(9) *Records usage, duplication and disclosure restrictions.* A description of any specific restrictions imposed by either the source agency or by statute or regulation on collateral uses of the records used in the matching program. Recipient agencies may not use the records obtained for a matching program under a matching agreement for any other purpose unless there is a specific statutory authority or there is a direct essential connection to the conduct of the matching program. Agreements shall specify how long the recipient agency may keep records provided for a matching program and

when they will be returned to the source agency or destroyed.

(10) *Records accuracy assessments.* A description of any information relating to the quality of the records to be used in the matching program such as the error rate percentage of the data entry for the affected records. The worse the quality of the data, the less likely the matching program will have a cost-beneficial result.

(11) *Disclosure Accounting.* A certification by the agency participating in a matching program as a source agency for disclosures outside the Department of Defense that a disclosure accounting shall be maintained on the subjects of record as required by the Privacy Act.

(12) *Access by the Comptroller General.* A statement that the Comptroller General may have access to all records of a recipient DoD component or non-Federal agency necessary to monitor or verify compliance with the agreement. In this instance, the Comptroller General may inspect state or local government records used in matching programs.

(c) *Non-Federal agencies.* Non-Federal agencies intending to participate in covered matching programs are required to do the following:

(1) Execute matching agreements prepared by a Federal agency or agencies involved in the matching program.

(2) Provide data to Federal agencies on the costs and benefits of matching programs.

(3) Certify that they will not take adverse action against an individual as a result of any information developed in a matching program unless the information has been independently verified and until the applicable number of days after the individual has been notified of the findings and given an opportunity to contest them has elapsed.

(4) For renewals of matching programs, certify that the terms of the agreement have been followed.

(d) *Duration of matching programs.* Matching agreements will remain in force only as long as necessary to fulfill their specific purposes. They will automatically expire 18 months after their approval unless the Defense Data Integrity Board grants an extension of up to one year at least three months prior to the actual expiration date. The

program must remain unchanged if an extension is to be granted. Each party to the agreement must certify that the program has been conducted in compliance with the matching agreement. Requests for extensions shall be submitted through channels to the Board.

(e) *Altered matching program.* (1) An altered matching program is one that is already established, but with such a significant change proposed that it requires revision of the matching notice and approval of the Defense Data Integrity Board, OMB and Congress. A significant change is one which does one or more of the following:

(i) Changes the purpose for which the program was established.

(ii) Changes the matching population either by including new categories of subjects of record, or by greatly increasing the numbers of records matched.

(iii) Changes the legal authority under which the match was being conducted.

(iv) Changes the records (data elements) that will be used in the match.

(2) A proposal to alter an established matching program shall be submitted through channels to the Defense Data Integrity Board for review and approval.

(f) *Non compliance sanctions.* (1) The agency shall not disclose any record for use in a matching program as a source agency to any recipient agency (within or outside the Department of Defense) if there is reason to believe that the terms of the matching agreement/MOU or the due process requirements are not being met by the recipient agency. The Defense Privacy Office, DA&M, shall be informed immediately, through channels, should any such incident occur. Normally consulting with the recipient agency should resolve the problem, but the responsibility rests with the source.

(2) No source agency shall renew a matching agreement/MOU unless the recipient agency (within or outside the Department of Defense) has certified that it has complied with the provisions of the agreement/MOU and the agency has no reason to believe otherwise.

(3) A willful disclosure of records from a system of records for any unau-

thorized computer matching program may subject the responsible officer or employee to criminal penalties. Civil remedies are also available to matching program subjects who can show they were harmed by an agency's violation of the Act as set forth in subpart J of this part.

§ 317.97 Cost-benefit analysis.

(a) *Purpose.* The requirement for a cost-benefit analysis by the Act is to assist the agency in determining whether or not to conduct or participate in a matching program. Its application is required in two places: As an agency conclusion in the matching agreement containing the justification and specific estimate of savings; and in the Data Integrity Board review process where it is forwarded as part of the matching proposal. The intent of this requirement is not to create a presumption that when agencies balance individual rights and cost savings, the latter should inevitably prevail. Rather, it is to ensure that sound management practices are followed when agencies use records from Privacy Act systems in matching programs. It is not in the government's interest to engage in matching activities that drain agency resources that could be better spent elsewhere. Agencies should use the cost-benefit requirement as an opportunity to re-examine programs and weed out those that produce only marginal results.

(b) *Cost-benefit analysis.* The agency, when proposing matching programs, must provide the Board with all information which is relevant and necessary to allow the Board to make an informed decision including a cost-benefit analysis. The Defense Data Integrity Board shall not approve any matching agreement unless the Board finds the cost-benefit analysis demonstrates the program is likely to be cost effective.

(1) The Board may waive the cost-benefit analysis requirement if it determines in writing that submission of such an analysis is not required.

(2) If a matching program is required by a specific statute, then a cost-benefit analysis is not required. However, any renegotiation of such a matching agreement shall be accompanied by a

cost-benefit analysis. The finding need not be favorable. The intent, in this case, is to provide Congress with information to help it evaluate the effectiveness of statutory matching requirements.

(3) The Board must find that agreements conform to the provisions of the Act and appropriate guidelines, regulations, and statutes.

§ 317.98 Appeals of denials of matching agreements.

(a) *Disapproval by the Board.* If the Defense Data Integrity Board disapproves a matching agreement, a party to the agreement may appeal the disapproval to the Director of the Office of Management and Budget, Washington, DC 20503. Appeals must be made within 30 days after the Defense Data Integrity Board's written disapproval. The appealing party shall submit with its appeal the following:

(1) Copies of all documentation accompanying the initial matching agreement proposal.

(2) A copy of the Defense Data Integrity Board's disapproval and reasons.

(3) Evidence supporting the cost-benefit effectiveness of the match.

(4) Any other relevant information, e.g., timing considerations, public interest served by the match, etc.

(b) *OMB approval.* If the Director of the Office of Management and Budget approves a matching program it will not become effective until 30 days after the Director reports his decision to Congress.

(c) *Recourse by the Inspector General.* If the Defense Data Integrity Board and the Director of the Office of Management and Budget both disapprove a matching program proposed by the Inspector General of the denial agency, the Inspector General may report that disapproval to the head of Department of Defense and to the Congress.

§ 317.99 Proposals for matching programs.

(a) *Who initiates the action.* The recipient DoD component (or the DoD component source agency in a match conducted by a non-Federal agency); or the recipient activity within the DoD component for internal matches, is re-

sponsible for reporting the match for Board approval. The responsible official should contact the other participants to gather the information necessary to make a unified report.

(b) *New or altered matching programs.* Determine if the match is a new program or an existing one. A new match is one for which no public notice has been published in the FEDERAL REGISTER. An altered matching program is an established (published public notice) match with such a significant change that it requires amendment. An altered matching program should not be confused with a request for an unchanged extension of an established program.

(c) *Contents of report (original and one copy).* (1) A proposed new matching program report shall consist of an agency letter of transmittal with the following attached documents:

(i) Completed agreement between the participants.

(ii) Benefit/cost analysis.

(iii) Proposed FEDERAL REGISTER matching notice for public review and comment.

(iv) Copies of all the appropriate forms (e.g., applications) of the participating parties providing direct notice to the individual or any other means of communication used.

(v) Copy or copies of the appropriate FEDERAL REGISTER system(s) of record notice(s) containing an appropriate routine use providing constructive notice to the individual.

(2) A report on a proposed alteration to an established matching program shall consist of an agency letter of transmittal with the following attached documents:

(i) A report containing the significant change(s) and the following additional information:

(A) What alternatives to matching the agencies considered and why a matching program was chosen.

(B) The date the match was approved by each participating Federal agency's Data Integrity Board.

(C) Whether a cost-benefit analysis was required and, if so, whether it projected a favorable ratio.

(ii) Proposed FEDERAL REGISTER matching notice for public review and comment.

(3) A report requesting an extension beyond 18 months of an established unchanged matching program must be received by the Defense Privacy Office, DA&M, at least four months prior to the actual expiration date and consist of an agency letter of transmittal with the following attached:

(i) Justification for the extension (not to exceed one year).

(ii) Certification by the participants that the program has been conducted in compliance with the matching agreement.

(d) *Who receives the reports.* All reports shall be submitted to, and reviewed by, the agency Privacy Advisor and forwarded to the Defense Privacy Office, DA&M, for consideration by the Defense Data Integrity Board.

(e) *Action by the Defense Privacy Office.* The Defense Privacy Office, DA&M, shall present proposals before the Defense Data Integrity Board which shall either approve or disapprove proposals on their merits. Any inaction based on insufficient data, justification, or supporting documentation shall be returned for any further corrective action deemed necessary. Any disapproved proposals are returned with the stated reasons. Board approved proposals are coordinated with the Office of the Assistant Secretary of Defense (Legislative Affairs) and the Office of the General Counsel, Department of Defense. The Defense Privacy Office prepares for the signature of the Chairman of the Board (Director of Administration and Management (DA&M)), transmittal letters sent to Congress and OMB and concurrently submits the proposed FEDERAL REGISTER matching notice for publication.

(f) *Time restrictions on the initiation of new or altered matching programs.* (1) All time periods begin from the date the Chairman of the Board signs the transmittal letters.

(2) At least 30 days must elapse before the matching program may become operational.

(3) The 30 day period for OMB and Congressional review and the 30 day notice and comment period for the Matching Notice may run concurrently.

(g) *Requests for waivers.* The agency may seek waivers of certain matching program requirements including the 30 day review period by OMB and Congress. Requests for waivers shall be included in the letter of transmittal to the report. Such requests shall cite the specific provision for which a waiver is being requested with full justification showing the reasons and the adverse consequences if a waiver is not granted.

(h) *Outside review and activity.* The agency may presume OMB and Congressional concurrence if the review period has run without comment from any reviewer outside the Department of Defense. Under no circumstances shall the matching program be implemented before 30 days have elapsed after publication of the matching notice in the FEDERAL REGISTER. This period cannot be waived.

Subpart J—Enforcement Actions

§ 317.110 Administrative remedies.

An individual who alleges he or she has been affected adversely by a violation of the Privacy Act shall be permitted to seek relief from the Assistant Director, Resources, through proper administrative channels.

§ 317.111 Civil court actions.

After exhausting all administrative remedies, an individual may file suit (5 U.S.C 552a(y)) in the Federal court against the agency for any of the following acts:

(a) *Denial of an amendment request.* The Assistant Director, Resources, or designee refuses the individual's request for review of the initial denial of an amendment or, after review, refuses to amend the record.

(b) *Denial of access.* The agency refuses to allow the individual to review the record or denies his or her request for a copy of the record.

(c) *Failure to meet recordkeeping standards.* The agency fails to maintain the individual's record with the accuracy, relevance, timeliness, and completeness necessary to assure fairness in any determination about the individual's rights, benefits, or privileges and, in

§317.112

fact, makes an adverse determination based on the record.

(d) *Failure to comply with the Privacy Act.* The agency fails to comply with any other provision of the Privacy Act or any rule or regulation promulgated under the Privacy Act and thereby causes the individual to be adversely affected.

§317.112 Criminal penalties.

The Privacy Act (5 U.S.C. 552a(i)) authorizes three criminal penalties against individuals. All three are misdemeanors punishable by fines of \$5,000.

(a) *Wrongful disclosure.* Any member or employee of the agency who, by virtue of his or her employment or position, has possession of or access to records and willfully makes a disclosure to anyone not entitled to receive the information.

(b) *Maintaining unauthorized records.* Any member or employee of the agency who willfully maintains a system of records for which a notice has not been published.

(c) *Wrongful requesting or obtaining records.* Any person who knowingly and willfully requests or obtains a record concerning an individual from the agency under false pretenses.

§317.113 Litigation status report.

Whenever a civil complaint citing the Privacy Act is filed against the agency in Federal court or whenever criminal charges are brought against an individual in Federal court (including referral to a court-martial) for any offense, the agency shall notify the Defense Privacy Office, DA&M. The litigation status report included in appendix C to this part provides a format for this notification. An initial litigation status report shall be forwarded providing, as a minimum, the information specified. An updated litigation status report shall be sent at each stage of litigation. When the court renders a formal disposition of the case, copies of the court's action, along with the litigation status report reporting the action, shall be sent to the Defense Privacy Office, DA&M.

32 CFR Ch. I (7-1-99 Edition)

§317.114 Annual review of enforcement actions.

(a) *Annual review.* The agency shall review annually the actions of its personnel that have resulted in either the agency being found civilly liable or an agency member being found criminally liable under the Privacy Act.

(b) *Reporting results.* The agency shall be prepared to report the results of the annual review to the Defense Privacy Office, DA&M.

Subpart K—Reports

§317.120 Report requirements.

(a) *Statutory requirements.* Subsection (p) of the Privacy Act requires a report and assigns to the Office of Management and Budget the responsibility for compiling the report.

(b) *OMB requirements.* (1) In addition to the report, the Office of Management and Budget requires that all agencies be prepared to report the results of the reviews.

(2) All reports of the agency concerning implementation of the Privacy Act shall be submitted to the Defense Privacy Office, DA&M, which shall prescribe the contents and suspense for such reports.

§317.121 Reports.

(a) *Submission to the Defense Privacy Office.* The agency shall prepare statistics and other documentation for the preceding calendar year concerning those items prescribed for the annual report and any reports of the reviews required, and when directed, send them to the Defense Privacy Office, DA&M.

(b) *Report Control Symbol.* Unless otherwise directed, any report concerning implementation of the Privacy Program shall be assigned Report Control Symbol DD-DA&M(A)1379.

(c) *Content of annual report.* The Defense Privacy Office, DA&M, shall prescribe the content of the annual report but, at a minimum, the annual report shall contain the following:

(1) Name and address of reporting agency.

(2) Name and telephone number of agency official who can best answer questions about this report.

- (3) Agency Privacy Act Officials.
 - (i) Senior Agency Official.
 - (ii) Privacy Act Officer.
- (4) If your agency was involved in any litigation involving the Privacy Act.
 - (i) Provide a citation to the case and a brief description of the background, issues and results.
 - (ii) If the cases required your agency to change its practices, describe how.
- (5) Systems of Records Inventory:
 - (i) Total number of systems of records as of December 31, 19XX.
 - (ii) Number of exempt systems.
 - (iii) Number of automated systems (either in whole or part).
 - (iv) Number of systems deleted.
 - (v) Number of systems added.
 - (vi) Number of routine uses added.
 - (vii) Number of routine uses deleted.
 - (viii) Number of existing systems to which an exemption(s) was added, and
 - (ix) Number of new systems to which an exemption(s) was added.
- (6) If your agency received any public comments on any of its systems of other Privacy Act implementing activities, briefly describe:
- (7) Access requests (first party requests which cited the Privacy Act):
 - (i) Number of requests.
 - (ii) Number granted in whole or in part.
 - (iii) Number denied in whole.
 - (iv) Number for which no record was found.
- (8) Amendment requests (first party requests which cited the Privacy Act):
 - (i) Number of requests.
 - (ii) Number granted in whole or part.
 - (iii) Number denied in whole.
- (9) Appeals of denial:
 - (i) Number of access denials appealed.
 - (ii) Number in which denial was upheld.
 - (iii) Number of amendment denials appealed.
 - (iv) Number in which denial was upheld.
- (10) Suggestions:

Subpart L—Agency Exemption Rules

§ 317.130 Establishing and using exemptions.

(a) *Types of exemptions.* (1) There are two types of exemptions permitted by the Privacy Act:

(i) General exemptions that authorize the exemption of a system of records from all but specifically identified provisions of the Privacy Act, and

(ii) Specific exemptions that allow a system of records to be exempted from only a few designated provisions of the Privacy Act.

(2) Neither the Privacy Act nor this part permits exemption of a system of records from all provisions of the Privacy Act.

(b) *Establishing exemptions.* (1) Neither general nor specific exemptions are established automatically for a system of records. Only the Director of DCAA or his/her designee shall make a determination that the system is one for which an exemption may be established and then propose and establish an exemption rule for the system. No system of records within the agency shall be considered exempted until the Assistant Director, Resources, DCAA has approved the exemption and an exemption rule has been published as a final rule in the FEDERAL REGISTER for this part.

(2) Only the Assistant Director, Resources, or his or her designee, may establish an exemption for a system of records.

(3) No exemption may be established for a system of records until the system itself has been established by publishing a notice in the FEDERAL REGISTER describing the system.

(4) A system of records is exempt from only those provisions of the Privacy Act that are identified specifically in the agency exemption rule for the system.

(c) *Provisions to which exemptions may be applied.* After, or along with, establishing the system of records, the Assistant Director, Resources, may establish an exemption rule that shall exempt the system of records from any

§317.131

32 CFR Ch. I (7-1-99 Edition)

provision of the Privacy Act for which an exemption is allowed.

(d) *Using exemptions.* (1) Exemptions should be used only for the specific purposes stated in the exemption rules and only when in the best interest of the Government. Exemptions should be applied to only the specific portions of the records that require protection.

(2) An exemption should not be used to deny an individual access to information that he or she can obtain under the FOIA.

(e) *Exempt records maintained in non-exempt systems.* (1) An exemption rule applies to the system of records for which it was established. If a record from an exempted system is incorporated intentionally into a system that has not been exempted, the published notice and rules for the non-exempted system will apply to the record and it will not be exempt from any provisions of the Privacy Act.

(2) A record from one DoD component's exempted system that is temporarily in the possession of another DoD component remains subject to the published system notice and rules of the originating DoD component. However, if the non-originating DoD component incorporates the record into its own system of records, the published notice and rules for the system into which it is incorporated shall apply. If that system of records has not been exempted, the record shall not be exempt from any provisions of the Privacy Act.

(3) Care should be exercised that exempt records are not accidentally misfiled into a system of records that are not exempted

§317.131 General exemptions.

(a) *Using general exemptions.* (1) DCAA is not authorized to establish the exemption for records maintained by the Central Intelligence agency under subsection (j)(1) of the Privacy Act.

(2) The general exemption provided by subsection (j)(2) of the Privacy Act may be established to protect criminal law enforcement records maintained by the agency.

(3) To be eligible for the (j)(2) exemption, the system of records must be maintained by an element that per-

forms, as one of its principal functions, the enforcement of criminal laws.

(4) Criminal law enforcement includes police efforts to detect, prevent, control, or reduce crime, or to apprehend criminals, and the activities of prosecution, court, correctional, probation, pardon, or parole authorities.

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

(i) Information compiled for the purpose of identifying criminal offenders and alleged criminal offenders consisting of only identifying data and notations of arrests; the nature and disposition of criminal charges; and sentencing, confinement, release, parole, and probation status.

(ii) Information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; and

(iii) Reports identifiable to an individual, compiled at any stage of the enforcement process, from arrest, apprehension, indictment, or prefferal of charges through final release from the supervision that resulted from the commission of a crime.

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

(i) Investigative records maintained by an element having no criminal law enforcement activity as one of its principal functions, or

(ii) Investigative records compiled by any element concerning individuals' suitability, eligibility, or qualification for duty, employment, or access to classified information, regardless of the principal functions of the DoD component that compiled them.

(7) The (j)(2) exemption established for a system of records maintained by a criminal law enforcement element cannot protect law enforcement records incorporated into a non-exempted system of records or any system of records maintained by an element not principally tasked with enforcing criminal laws. Agency system managers are prohibited to incorporate criminal law enforcement records into systems other than those maintained by criminal law enforcement elements.

(b) *Access to records under a (j)(2) exemption.* Requests for access to criminal law enforcement records maintained in a system for which a (j)(2) exemption has been established shall be processed as if also made under the FOIA.

§ 317.132 Specific exemptions.

(a) *Using specific exemptions.* Specific exemptions permit certain categories of records to be exempted from specific provisions of the Privacy Act. Subsections (k)(1-7) of the Privacy Act permits claiming exemptions for seven categories of records. To be eligible for a specific exemption, the record must meet the corresponding criteria.

(1) (k)(1) exemption: Information properly classified under DoD 5200.1-R¹¹ (32 CFR part 159) in the interest of national defense or foreign policy.

(2) (k)(2) exemption: Investigatory information compiled for law enforcement purposes. If maintaining the information causes an individual to be ineligible for or denied any right, benefit, or privilege that he or she would otherwise be eligible for or entitled to under Federal law, then he or she shall be given access to the information, except for the information that would identify a confidential source. The (k)(2) exemption, when established, allows limited protection of investigative records normally maintained in a (j)(2) exempt system for use in personnel and administrative actions.

(3) (k)(3) exemption: Records maintained in connection with providing protective services to the President of the United States and other individuals under 18 U.S.C. 3056.

(4) (k)(4) exemption: Records required by Federal law to be maintained and used solely as statistical records that are not used to make any determination about an identifiable individual, except as provided by 13 U.S.C. 8.

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

identity of a confidential source. This exemption allows protection of confidential sources in background investigations, employment inquiries, and similar inquiries used in personnel screening to determine suitability, eligibility, or qualifications.

(6) (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 testing or examination process.

(7) (k)(7) exemption: Evaluation material used to determine potential for promotion in the military services, but only to the extent that disclosure would reveal the identity of a confidential source.

(b) *Confidential source.* (1) A “confidential source” is defined under the Privacy Act as a person or organization that has furnished information to the Federal Government under an express promise or, before September 27, 1975, under an implied promise that the identity of the person or organization would be held in confidence.

(2) Promises of confidentiality are to be given on a limited basis and only when essential to obtain the information sought. Appropriate procedures should be established for granting confidentiality and designate those categories of individuals authorized to make such promises.

(c) *Access to records under specific exemptions.* Requests for access to records maintained in systems of records for which specific exemptions have been established shall be processed as if also made under the FOIA.

§ 317.133 DCAA exempt record systems.

(a) *Exempt systems of records.* The Director, DCAA has made a determination and claims an exemption for the following agency systems of records by publication of an appropriate exemption rule for the record system and therefore allowing the agency to invoke, at its discretion, the particular exemption permitted by the Privacy Act from certain subsections of the Privacy Act.

¹¹ See footnote 3 to § 317.1(b).

(b) *Classified material.* The Director, DCAA has made a determination that all systems of records maintained by the agency shall be exempt from 5 U.S.C. 552a(d) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1) to the extent that the record system contains any information properly classified under Executive Order 12958 and required by the executive order to be withheld in the interest of national defense or foreign policy. This blanket 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) *General exemption rules.* [Reserved]

(d) *Specific exemption rules.* [Reserved]

[57 FR 48992, Oct. 29, 1992, as amended at 61 FR 2916, Jan. 30, 1996]

APPENDIX A TO PART 317—DCAA BLANKET ROUTINE USES

A. LAW ENFORCEMENT ROUTINE USE

In the event that a system of records maintained by this agency to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether Federal, State, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

B. DISCLOSURE WHEN REQUESTING INFORMATION ROUTINE USE

A record from a system of records maintained by this agency may be disclosed as a routine use to a Federal, State, or local agency maintaining civil, criminal, or other relevant enforcement information, or other pertinent information, such as current licenses, if necessary to obtain information relevant to a agency decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

C. DISCLOSURE OF REQUESTED INFORMATION ROUTINE USE

A record from a system of records maintained by this agency may be disclosed to a

Federal Agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

D. CONGRESSIONAL INQUIRIES ROUTINE USE

Disclosure from a system of records maintained by this agency may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

E. PRIVATE RELIEF LEGISLATION ROUTINE USE

Relevant information contained in all systems of records of the agency published on or before August 22, 1975, may be disclosed to the Office of Management and Budget in connection with the review of private relief legislation as set forth in OMB Circular A-19 at any stage of the legislative coordination and clearance process as set forth in that circular.

F. DISCLOSURES REQUIRED BY INTER- NATIONAL AGREEMENTS ROUTINE USE

A record from a system of records maintained by this agency may be disclosed to foreign law enforcement, security, investigatory, or administrative authorities in order to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements, including those regulating the stationing and status in foreign countries of Department of Defense military and civilian personnel.

G. DISCLOSURE TO STATE AND LOCAL TAXING AUTHORITIES ROUTINE USE

Any information normally contained in IRS Form W-2 that is maintained in a record from a system of records maintained by this agency may be disclosed to State and local taxing authorities with which the Secretary of the Treasury has entered into agreements pursuant to Title 5 U.S.C. Sections 5516, 5517, 5520, and only to those State and local taxing authorities for which an employee or military member is or was subject to tax, regardless of whether tax is or was withheld. This routine use is in accordance with Treasury Fiscal Requirements Manual Bulletin No. 76-07.

H. DISCLOSURE TO THE OFFICE OF PERSONNEL MANAGEMENT ROUTINE USE

A record from a system of records subject to the Privacy Act and maintained by this

agency may be disclosed to the Office of Personnel Management concerning information on pay and leave, benefits, retirement reductions, and any other information necessary for the Office of Personnel Management to carry out its legally authorized Government-wide personnel management functions and studies.

I. DISCLOSURE TO THE DEPARTMENT OF JUSTICE FOR LITIGATION ROUTINE USE

A record from a system of records maintained by this agency may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the agency, or any officer, employee or member of the agency in pending or potential litigation to which the record is pertinent.

J. DISCLOSURE TO MILITARY BANKING FACILITIES OVERSEAS ROUTINE USE

Information as to current military addresses and assignments may be provided to military banking facilities that provide banking services overseas and that are reimbursed by the Government for certain checking and loan losses. For personnel separated, discharged, or retired from the Armed Forces, information as to last known residential or home of record address to the military banking facility upon certification by a banking facility officer that the facility has a returned or dishonored check negotiated by the individual or the individual has defaulted on a loan and that if restitution is not made by the individual, the U.S. Government will be liable for the losses the facility may incur.

K. DISCLOSURE OF INFORMATION TO THE GENERAL SERVICES ADMINISTRATION ROUTINE USE

A record from a system of records maintained by this agency may be disclosed as a routine use to the General Services Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. Sections 2904 and 2906.

L. DISCLOSURE OF INFORMATION TO THE NATIONAL ARCHIVES AND RECORDS ADMINISTRATION ROUTINE USE

A record from a system of records maintained by this agency may be disclosed as a routine use to the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. Sections 2904 and 2906.

M. DISCLOSURE TO THE MERIT SYSTEMS PROTECTION BOARD ROUTINE USE

A record from a system of records maintained by this agency may be disclosed as a routine use to the Merit Systems Protection

Board, including the Office of the Special Counsel, for the purpose of litigation, including administrative proceedings, appeals, special studies of the civil service and other merit systems, review of OPM or agency rules and regulations, investigation of alleged or possible prohibited personnel practices, including administrative proceedings involving any individual subject of a DoD investigation, and such other functions promulgated in 5 U.S.C. Section 1205 or as may be authorized by law.

N. COUNTERINTELLIGENCE PURPOSES ROUTINE USE

A record from a system of records maintained by this agency may be disclosed as a routine use outside the Department of Defense for the purpose of counterintelligence activities authorized by U.S. law or executive order or for the purpose of enforcing laws that protect the national security of the United States.

APPENDIX B TO PART 317—PROVISIONS OF THE PRIVACY ACT FROM WHICH A GENERAL OR SPECIFIC EXEMPTION MAY BE CLAIMED

Exemption		Section of the Privacy Act
(j)(2)	(k)(1-7)	
No	No	(b)(1) Disclosure within the Department of Defense
No	No	(b)(2) Disclosure to the public
No	No	(b)(3) Disclosure for a routine use
No	No	(b)(4) Disclosure to Bureau of Census
No	No	(b)(5) Disclosure for statistical research and reporting
No	No	(b)(6) Disclosure to National Archives
No	No	(b)(7) Disclosure for law enforcement purposes
No	No	(b)(8) Disclosure under emergency circumstances
No	No	(b)(9) Disclosure to Congress
No	No	(b)(10) Disclosure to General Accounting Office
No	No	(b)(11) Disclosure pursuant to court orders
No	No	(b)(12) Disclosure to consumer reporting agency
No	No	(c)(1) Making disclosure accountings
No	No	(c)(2) Retaining disclosure accountings
Yes	Yes	(c)(3) Making disclosure accounting available to the individual
Yes	No	(c)(4) Informing prior recipients of corrections
Yes	Yes	(d)(1) Individual access to records
Yes	Yes	(d)(2) Amending records
Yes	Yes	(d)(3) Review of the Component's refusal to amend a record
Yes	Yes	(d)(4) Disclosure of disputed information
Yes	Yes	(d)(5) Access to information compiled in anticipation of civil action
Yes	Yes	(e)(1) Restrictions on collecting information

Pt. 317, App. C

32 CFR Ch. I (7–1–99 Edition)

Exemption		Section of the Privacy Act
(j)(2)	(k)(1–7)	
Yes	No	(e)(2) Collecting directly from the individual
Yes	No	(e)(3) Informing individuals from whom information is requested
No	No	(e)(4)(A) Describing the name and location of the system
No	No	(e)(4)(B) Describe categories of individuals
No	No	(e)(4)(C) Describing categories of records
No	No	(e)(4)(D) Describing routine uses
No	No	(e)(4)(E) Describing records management policies and practices
No	No	(e)(4)(F) Identifying responsible officials
Yes	Yes	(e)(4)(G) Procedures for determining if a system contains a record on an individual
Yes	Yes	(e)(4)(H) Procedures for gaining access
Yes	Yes	(e)(4)(I) Describing categories of information sources
Yes	No	(e)(5) Standards of accuracy
No	No	(e)(6) Validating records before disclosure
No	No	(e)(7) Records of First Amendment activities
Yes	No	(e)(8) Notification of disclosures under compulsory legal process
No	No	(e)(9) Rules of conduct
No	No	(e)(10) Administrative, technical and physical safeguards
No	No	(e)(11) Notice of new and revised routine uses
Yes	Yes	(f)(1) Rules for determining if an individual is subject of a record
Yes	Yes	(f)(2) Rules for handling access requests
Yes	Yes	(f)(3) Rules for granting access
Yes	Yes	(f)(4) Rules for amending records
Yes	Yes	(f)(5) Rules regarding fees
Yes	No	(g)(1) Basis for civil action
Yes	No	(g)(2) Basis for judicial review and remedies for refusal to amend
Yes	No	(g)(3) Basis for judicial review and remedies for denial of access
Yes	No	(g)(4) Basis for judicial review and remedies for other failure to comply
Yes	No	(g)(5) Jurisdiction and time limits
Yes	No	(h) Rights legal guardians
No	No	(i)(1) Criminal penalties for unauthorized disclosure
No	No	(i)(2) Criminal penalties for failure to publish
No	No	(i)(3) Criminal penalties for obtaining records under false pretenses
Yes	No	(j) Rulemaking requirement
N/A	No	(j)(1) Federal exemption for the Central Intelligence Agency
N/A	No	(j)(2) General exemption for criminal law enforcement records
Yes	N/A	(k)(1) Exemption for classified material
N/A	N/A	(k)(2) Exemption for law enforcement material
Yes	Yes	(k)(3) Exemption for records pertaining to Presidential protection
Yes	N/A	(k)(4) Exemption for statistical record

Exemption		Section of the Privacy Act
(j)(2)	(k)(1–7)	
Yes	N/A	(k)(5) Exemption for investigatory material compiled for determining suitability for employment or service
Yes	N/A	(k)(6) Exemption for testing or examination material
Yes	N/A	(k)(7) Exemption for promotion evaluation materials used by the Armed Forces
Yes	No	(l)(1) Records stored in NARA records centers
Yes	No	(l)(2) Records archived before September 27, 1975
Yes	No	(l)(3) Records archived on or after September 27, 1975
Yes	No	(m) Applicability to government contractors
Yes	No	(n) Mailing lists
Yes	No	(o) Reports on new systems
Yes	No	(p) Biennial report (Note: Department of Defense requires an annual report)

[57 FR 48992, Oct. 29, 1992, as amended at 62 FR 26390, May 14, 1997]

APPENDIX C TO PART 317—LITIGATION STATUS REPORT

- (a) Case Name and number:
- (b) Plaintiff(s):
- (c) Defendant(s):
- (d) Basis for Court Action:
- (e) Initial Litigation:
 - (1) Date Complaint or Charges Filed:
 - (2) Court:
 - (3) Court Action:
 - (6) Appeal (if any):
 - (1) Date Appeal Filed:
 - (2) Court:
 - (3) Case Number:
 - (4) Court Ruling:
 - (g) Remarks:

PART 318—DEFENSE THREAT REDUCTION AGENCY (DTRA)

- Sec.
- 318.1 Purpose and scope.
- 318.2 Applicability.
- 318.3 Designations and responsibilities.
- 318.4 Procedures for requests pertaining to individual records in a record system.
- 318.5 Disclosure of requested information to individuals.
- 318.6 Request for correction or amendment to a record.
- 318.7 Agency review of request for correction or amendment of record.