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

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

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

(j) QNRO–4.

(1) *System name:* Freedom of Information Act and Privacy Act Files.

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

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

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

[65 FR 20372, Apr. 17, 2000, as amended at 66 FR 41783, Aug. 9, 2001; 66 FR 54926, Oct. 31, 2001; 67 FR 17616, Apr. 11, 2002]

PART 327—DEFENSE COMMISSARY AGENCY PRIVACY ACT PROGRAM

Sec.

AUTHORITY: Pub. L. 93–579, 88 Stat. 1896 (5 U.S.C. 522a).

SOURCE: 65 FR 39806, June 28, 2000, unless otherwise noted.

§ 327.1 Purpose.

This part implements the basic policies and procedures for the implementation of the Privacy Act of 1974, as amended (5 U.S.C. 552a); OMB Circular A–130;[1] and 32 CFR part 310; and to promote uniformity in the DeCA Privacy Act Program.

§ 327.2 Applicability.

This part applies to Headquarters, Field Operating Activities (FOA), Regions, Zones, Central Distribution Centers (CDC), Commissaries of DeCA, and contractors during the performance of a contract with DeCA. All personnel are expected to comply with the procedures established herein.

§ 327.3 Responsibilities.

(a) *The Director, DeCA.* (1) Supervises the execution of the Privacy Act and this part within the DeCA, and serves as the DeCA Privacy Act Appeal Authority.

(2) Appoints:

(i) The Executive Director for Support as the DeCA Initial Denial Authority for the DeCA Privacy Act Program.

(ii) The Records Manager, Office of Safety, Security, and Administration as the DeCA Privacy Act Officer.

(b) *The Privacy Act Officer, DeCA.* (1) Establishes and manages the PA program for DeCA.

(2) Provides guidance, assistance and training.

(3) Controls and monitors all requests received and prepares documentation to the office of primary responsibility (OPR) for response.

(4) Prepares response to requester based on information provided by the OPR.

(5) Signs all response requests for releasable information to the requester after coordination through the General Counsel. Ensures that all denied requests for information are released by the DeCA Initial Denial Authority.

(6) Publishes instructions to contractors that:

(i) Provide DeCA Privacy program guidance to their personnel who solicit, award, or administer government contracts;

(ii) Inform prospective contractors of their responsibilities regarding the DeCA Privacy Program; and

(iii) Establish an internal system of contractor performance review to ensure compliance with DeCA's Privacy program.

(iv) Prepare and submit System Notices to the Defense Privacy Office for publication in the FEDERAL REGISTER.

(7) Maintain Privacy Case files and records of disclosure accounting.

(8) Submit the DeCa Annual Privacy Act Report (RCS: DD–DA&M(A)1379) to the Defense Privacy Office.

(c) *DeCA Directorates/Staff Offices.* (1) Provide response and the information requested to the PA Officer for release to the individual.

(2) In the event the information is to be denied release, the requested information and rationale for denial will be forwarded to the PA Officer for denial determination.

(d) *Regions.* Regional Directors will appoint a Regional PA Coordinator who will maintain suspense control of PA actions, prepare documentation to the OPR for response, forward the information to the DeCA PA Officer for release determination, and notify the requester that the response will be received from the DeCA PA Officer using the format in Appendix A to this part.

(e) *DeCA Field Operating Activities (FOAs).* (1) Upon receipt of a PA request that has not been received from the DeCA PA Officer, notify the DeCA PA Officer within 2 days.

(2) Collect all information available and forward to the DeCA PA Officer. If the requested information is not available, provide the DeCA PA Officer the rationale to respond to the requester.

(f) *Central Distribution Centers (CDCs) and Commissaries.* (1) Upon receipt of a PA request, not received from the Region Coordinator, notify the Region Coordinator within 2 days.

(2) Collect all information available and forward it to the Region Coordinator for submission to DeCA PA Officer. If requested information is not available, provide the Region Coordinator the rationale so they can prepare a response to the DeCA PA Officer. If

[1] Copies may be obtained: http://www.whitehouse.gov/OMB/circulars.

the information is available but determined to be exempt, provide the Region Coordinator with the requested information and specific reasons why the request should be denied. The Region Coordinator will formalize a reply to the DeCA PA Officer, forwarding requested information and reasons for denial. The DeCA PA Officer will prepare the response to the requester with coordination by the General Counsel and signature by the IDA.

§ 327.4 Definitions.

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

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 is considered an agency within the meaning of the Privacy Act.

Computer room. Any combination of electronic hardware and software integrated in a variety of forms (firmware, programmable software, hard wiring, or similar equipment) that permits the processing of textual data. The equipment contains device to receive information and other processors with various capabilities to manipulate the information, store and provide input.

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

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

Federal Register system. Established by Congress to inform the public of interim, proposed, and final regulations or rulemaking documents having substantial impact on the public. In this case, DeCA directives have the same meaning as regulations or rulemaking documents. The secondary role of the Federal Register system is to publish notice documents of public interest.

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

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

Law enforcement activity. Any activity engaged in the enforcement of criminal laws, including efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities.

Maintain. Includes maintain, collect, use or disseminate.

Official use. Within the context of this part, this term is used when officials and employees of a DoD Component have a demonstrated need for the use of any record or the information contained therein in the performance of their official duties, subject to DoD 5200.1–R,[2] ''DoD Information Security Program Regulation.''

Personal information. Information about an individual that identifies, relates or is unique to, or describes him or her; *e.g.,* a social security number, age, military rank, civilian grade, marital status, race, salary, home/office phone numbers, etc.

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

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.

[2] Copies may be obtained: http//www.whs.osd.mil/corres.htm.

Member of the public. Any individual or party acting in a private capacity to include federal employees or military personnel.

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

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.

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

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.

System manager. The DoD Component official who is responsible for the operation and management of a system of records.

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

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 or graphic presentations intended to communicate verbally or visually with another individual.

Word processing equipment. Any combination of electronic hardware and computer software integrated in a variety of forms (firmware, programmable software, hard wiring, or similar equipment) that permits the processing of textual data. Generally, the equipment contains a device to recieve information, a computer-like processor with various capabilities to manipulate the information, a storage medium, and an output device.

§ 327.5 Systems of records.

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

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

(2) Be under the control of DeCA.

(b) *Retrieval practices.* Records in a group of records that may be retrieved by a name or personal identifier are not covered by this part even if the records contain personal data and are under the control of DeCA. The records MUST BE, in fact, retrieved by name or other personal identifier to become a system of records for DeCA.

(c) *Relevance and necessity.* Only those records that contain personal information which is relevant and necessary to accomplish a purpose required by Federal statute or an Executive Order will be maintained by DeCA.

(d) *Authority to establish systems of records.* Director, DeCA has the authority to establish systems of records; however, each time a system of records is established, the Executive Order or Federal statute that authorizes maintaining the personal information must be identified.

(1) DeCA will not maintain any records describing how an individual exercises his or her rights guaranteed by the First Amendment of the U.S. Constitution.

(2) These 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.

(e) *System manager's evaluation.* Systems managers, along with the DeCA Privacy Officer, shall evaluate the information to be included in each new system before establishing the system

and evaluate periodically the information contained in each existing system of records for relevancy and necessity. Such a review will also occur when a system notice amendment or alteration is prepared. Consider the following:

(1) The relationship of each item of information retained and collected to the purpose for which the system is maintained.

(2) The specific impact on the purpose or mission of not collecting each category of information contained in the system.

(3) The possibility of meeting the informational requirements through use of information not individually identifiable or through other techniques, such as sampling.

(4) The length of time each item of personal information must be retained.

(5) The cost of maintaining the information.

(6) The necessity and relevancy of the information to the purpose for which it was collected.

(f) *Discontinued information requirements.* (1) When notification is received to stop collecting any category or item of personal information, the DeCA PA Officer will issue instructions to stop immediately and also excise this information from existing records, when feasible, and amend existing notice.

(2) Disposition of these records will be provided by the DeCA PA Officer in accordance with the DeCA Filing System.[3]

(g) *Government contractors.* (1) When DeCA contracts for the operation or maintenance of a system of records or a portion of a system of records by a contractor, the record system or the portion affected are considered to be maintained by DeCA and are subject to this part. DeCA is responsible for applying the requirements of this part to the contractor. The contractor and its employees are to be considered employees of DeCA for the purposes of the approved provisions of the Privacy Act during the performance of the contract. Consistent with the Defense Acquisition Regulation, contracts requiring the maintenance of a system of records or the portion of a system of records shall identify specifically the record system and the work to be performed and shall include in the solicitation and resulting contract such terms as are prescribed in the Defense Acquisition Regulation (DAR).[4]

(2) If the contractor must use or have access to individually identifiable information subject to this part to perform any part of a contract, and the information would have been collected and maintained by DeCA but for the award of the contract, these contractor activities are subject to this part.

(3) The restrictions in paragraphs (g)(1) and (g)(2) of this section do not apply to records:

(i) Established and maintained to assist in making internal contractor management decisions such as those maintained for use in managing the contract.

(ii) Those maintained as internal contractor employee records even when used in conjunction with providing goods and services to DeCA.

(4) Disclosure of records to contractors. Disclosure of personal records to a contractor for the use in the performance of any DeCA contract is considered a disclosure within the Department of Defense (DoD). The contractor is considered the agent of DeCA and is to be maintaining and receiving the records for DeCA.

(h) *Safeguarding personal information.* DeCA personnel will protect records in every system of records for confidentiality against alteration, unauthorized disclosure, embarrassment, or unfairness to any individual about when information is kept.

(1) Supervisor/Manager paper records maintained by DeCA personnel will be treated as 'For Official Use Only' (FOUO) documents and secured in locked file cabinets, desks or bookcases during non-duty hours. During normal working hours, these records will be out-of-sight if the working area is accessible to non-government personnel.

(2) Personnel records maintained by DeCA computer room or stand alone systems, will be safeguarded at all

[3] Copies may be obtained: Defense Commissary Agency, ATTN: FOIA/Privacy Officer, 1300 E. Avenue, Fort Lee, VA 23801–1800.

[4] See footnote 3 to § 327.5.

times. Printed computer reports containing personal data must carry the markings FOUO. Other media storing personal data such as tapes, reels, disk packs, etc., must be marked with labels which bear FOUO and properly safeguarded.

(3) Adherence to paragraphs (h)(1) and (h)(2) of this section, fulfills the requirements of 32 CFR part 285.

(i) *Records disposal.* (1) DeCA records containing personal data will be shredded or torn to render the record unrecognizable or beyond reconstruction.

(2) The transfer of large quantities of DeCA records containing personal data to disposal activities is not considered a release of personal information under this part. The volume of such transfers makes it difficult or impossible to identify easily specific individual records. Care must be exercised to ensure that the bulk is maintained so as to prevent specific records from becoming readily identifiable. If the bulk is amintained, no special procedures are required. if the bulk cannot be maintained, dispose of the records by shredding or tearing to render the record unrecognizable or beyond reconstruction.

§ 327.6 Collecting personal information

(a) *Collect directly from the individual.* To the greatest extent practicable, collect personal information directly from the individual to whom it pertains if the information may be used in making any determination about the rights, privileges, or benefits of the individual under any Federal program.

(b) *Collecting personal information from third parties.* It may not be practical to collect personal information directly from an individual in all cases. Some examples of this are:

(1) Verification of information through third party sources for security or employment suitability determinations;

(2) Seeking third party opinions such as supervisory comments as to job knowledge, duty performance, or other opinion-type evaluations;

(3) When obtaining the needed information directly from the individual is exceptionally difficult or may result in unreasonable costs; or

(4) Contacting a third party at the request of the individual to furnish certain information such as exact periods of employment, termination dates, copies of records, or similar information.

(c) *Collecting social security numbers (SSNs).* (1) It is unlawful for DeCA to deny an individual any right, benefit, or privilege provided by law because an individual refuses to provide his or her SSN. Executive Order 9397 authorizes solicitation and use of SSNs as numerical identifiers for individuals in most Federal record systems, however, it does not provide mandatory authority for soliciting.

(2) When an individual is requested to provide their SSN, they must be told:

(i) the uses that will be made of the SSN;

(ii) The statute, regulation or rule authorizing the solicitation of the SSN; and

(iii) Whether providingthe SSN is voluntary or mandatory.

(3) Once the SSN has been furnished for the purpose of establishing a record, the notification in paragraph (c)(2) of this section is not required if the individual is only requested to furnish or verify the SSNs for identification purposes in connection with the normal use of his or her records.

(d) *Privacy act statements.* When a DeCA individual is requested to furnish personal information about himself or herself for inclusion in a system of records, a Privacy Act Statement is required regardless of the medium used to collect the information, *e.g.* forms, personal interviews, telephonic interviews. The statement allows the individual to make a decision whether to provide the information requested. The statement will be concise, curent, and easily understood and must state whether providing the information is voluntary or mandatory. if furnishing the data is mandatory, a Federal statute, Executive Order, regulation or other lawful order must be cited. If the personal information solicited is not to be incorporated into a DeCA system of records, a PA statement is not required. This information obtained without the PA statement will not be incorporated into any DeCA systems of records.

(1) *The DeCA Privacy Act Statement will include:*

(i) The specific Federal statute or Executive Order that authorized collection of the requested information;

(ii) The principal purpose or purposes for which the information is to be used;

(iii) The routine uses that will be made of the information;

(iv) Whether providing the information is voluntary or mandatory; and

(v) The effects on the individual if he or she chooses not to provide the requested information.

(2) *Forms.* When DeCA uses forms to collect personal information, placement of the Privacy Act advisory statement should be in the following order of preference:

(i) Below the title of the form and positioned so the individual will be advised of the requested information,

(ii) Within the body of the form with a notation of its location below the title of the form,

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

(iv) Attached to the form as a tear-off sheet, or

(v) Issued as a separate supplement to the form.

(3) *Forms issued by non-DoD Activities.* Ensure that the statement prepared by the originating agency on their forms is adequate for the purpose for which DeCA will use the form. If the statement is inadequate, DeCA will prepare a new statement before using the form. Forms issued by other agencies not subject to the Privacy Act but its use requires DeCA to collect personal data, a Privacy Act Statement will be added.

§ 327.7 Access by individuals

(a) *Individual access to personal information.* Release of personal information to individuals whose records are maintained in a systems of records under this part is not considered public release of information. DeCA will release to the individuals all of the personal information, except to the extent the information is contained in an exempt system of records.

(1) *Requests for access.* (i) Individuals in DeCA Headquarters and FOAs will address requests for access to their personal information to the DeCA Privacy Act Officers. Individuals in Regions, CDCs, and commissaries, will address requests to their respective Region Privacy Act Coordinator. The individual is not required to explain or justify why access is being sought.

(ii) If an individual wishes to be accompanied by a third party when seeking access to his or her records or to have the records released directly to the third party, a signed access authorization granting the third party access is required.

(iii) A DeCA individual will not be denied access to his or her records because he or she refuses to provide his or her SSN unless the SSN is the only way retrieval can be made.

(2) *Granting access.* (i) If the record is not part of an exempt system, DeCA personnel will be granted access to the original record or an exact copy of the original record without any changes or deletions. Medical records will be disclosed to the individual to whom they pertain unless an individual fails to comply with the established requirements. This includes refusing to name a physician to receive medical records when required, refusing to pay fees, or when a judgment is made that access to such records may have an adverse effect on the mental or physical health of the individual. Where an adverse effect may result, a release will be made in consultation with a physician.

(ii) DeCA personnel may be denied access to information compiled in reasonable anticipation of a civil action or proceeding. The term ''civil proceeding'' is intended to include quasi-judicial and pretrial judicial proceedings. Information prepared in conjunction with the quasi-judicial, pretrial and trial proceedings to include those prepared by DeCA legal and non-legal officials of the possible consequences of a given course of action are protected from access.

(iii) Requests by DeCA personnel for access to investigatory records pertaining to themselves, compiled for law enforcement purposes, are processed under this part and that of 32 CFR part 310. Those requests by DeCA personnel for investigatory records pertaining to themselves that are in records systems exempt from access provisions shall be processed under this part or 32 CFR part 285, depending upon which provides the greatest degree of access.

(3) *Non agency records.* (i) Uncirculated personal notes and records that are not given or circulated to any person or organization (example, personal telephone list) that are kept or discarded at the author's discretion and over which DeCA exercises no direct control, are not considered DeCA records. However, if personnel are officially directed or encouraged, either in writing or orally, to maintain such records, they may become ''agency records'' and may be subject to this part.

(ii) Personal uncirculate handwritten notes of team leaders, office supervisors, or military supervisory personnel concerning subordinates are not a system of records within the meaning of this part. Such notes are an extension of the individual's memory. These notes, however, must be maintained and discarded at the discretion of the individual supervisor and not circulated to others. Any established requirement to maintain such notes (written or oral directives, regulation or command policy) make these notes ''AGENCY RECORDS.'' If the notes are circulated, they must be made a part of the system of records. Any action that gives personal notes the appearance of official agency records is prohibited unless they have been incorporated into a DeCA system of records.

(b) *Relationship between the Privacy Act and the Freedom of Information Act (FOIA).* (1) Requests from DeCA individuals for access to a record pertaining to themselves made under the FOIA are processed under the provisions of this part, 32 CFR part 310 and DeCA Directive 30–12, Freedom of Information Act (FOIA) Program.[5]

(2) Request from DeCA individuals or access to a record pertaining to themselves are processed under this part and 32 CFR part 310.

(3) Requests from DeCA individuals for access to records about themselves that cite both Acts or the DeCA implementing directives for both Acts are processed under this part except:

(i) When the access provisions of the FOIA provide a greater degree of access process under the FOIA, or

(ii) When access to the information sought is controlled by another Federal statute process access procedures under the controlling statute.

(4) Requests from DeCA individuals for access to information about themselves in a system of records that do not cite either Act or DeCA implementing directive are processed under the procedures established by this part.

(5) DeCA requesters will not be denied access to personal information concerning themselves that would be releasable to them under either Act because they fail to cite either Act or the wrong Act. The Act or procedures used in granting or denying access will be explained to requesters.,

(6) DeCA requesters should receive access to their records within 30 days.

(7) Records in all DeCA systems maintained in accordance with the Government-wide systems notices are in temporary custody of DeCA, and all requests or amend these records will be processed in accordance with this part.

(c) *Denial of individual access.* (1) A DeCA individual may be denied formal access to a record pertaining to him/her only if the record:

(i) Was compiled in reasonable anticipation of civil action.

(ii) Is in a system of records that has been exempt from access provisions of this part.

(iii) All systems of records maintained by the Defense Commissary Agency shall be exempt from the requirements of 5 U.S.C. 552a(d) pursuant to 5 U.S.C. 552a(k)(1) to the extent that the system contains any information properly classified under Executive Order 12958 and which is required by the Executive Order to be withheld in the interest of national defense 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 herein may contain items of information that have been properly classified.

(iv) Is contained in a system of records for which access may be denied under some other Federal statute.

(v) All systems of records maintained by the DeCA shall be exempt from the requirements of 5 U.S.C. 552a(d) pursuant to 5 U.S.C. 552a(k)(1) to the extent

[5] See footnote 3 to § 327.5.

that the system contains any information properly classified under Executive Order 12958 and which is required by the Executive Order to be withheld in the interest of national defense of foreign policy. This exemption, which may be applicable to parts of all systems of records, is necessary because certain record systems not otherwise specifically designated for exemptions herein may contain items of information that have been properly classified.

(2) DeCA individuals will only be denied access to those portions of the records from which the denial of access serves some legitimate governmental purpose.

(3) Other reasons to refuse DeCA individuals are:

(i) The request is not described well enough to locate it within a reasonable amount of effort by the PA Officer or PA Coordinator; or

(ii) An individual fails to comply with the established requirements including refusing to name a physician to receive medical records when required or to pay fees.

(4) Only the DeCA IDA can deny access. This denial must be in writing and contain:

(i) The date of the denial, name, title of position, and signature of the DeCA Initial Denial Authority.

(ii) The specific reasons for the denial, including specific reference to the appropriate sections of the PA, other statutes, this part or the Code of Federal Regulations (CFR);

(iii) Information providing the right to appeal the denial through the DeCa appeal procedure within 60 days, and the title, position and address of the DeCA PA Appellate Authority.

(5) *DeCA Appeal Procedures*. The Director of DeCA, or the designee, will review any appeal by an individual from a denial of access to DeCA records. Formal written notification will be provided to the individual explaining whether the denial is sustained totally or in part. The DeCA PA Officer will:

(i) Assign a control number and process the appeal to the Director, DeCA or the designee appointed by the Director.

(ii) Provide formal written notification to the individual by the appeal authority explaining whether the denial is sustained totally or in part and the exact reasons for the denial to include provisions of the Act, other statute, this part or the CFR whichever the determination is based, or

(iii) Provide the individual access to the material if the appeal is granted.

(iv) Process all appeals within 30 days of receipt unless the appeal authority determines the review cannot be made within that period and provide notification to the individual the reasons for the delay and when an answer may be expected.

(d) *Amendment of records*. (1) DeCA employees are encouraged to review the personal information being maintained abut them periodically. An individual may request amendment of any record contained in a system of records unless the system of records has been exempt specifically from the amendment procedures by the Director, DeCa. A request for amendment must include:

(i) A description of the item or items to be amended.

(ii) The specific reason for the amendment.

(iii) The type of amendment action such as deletion, correction or addition.

(iv) Copies of evidence supporting the request.

(v) DeCA employees may be required to provide identification to make sure that they are indeed seeking to amend a record pertaining to themselves.

(2) The amendment process is not intended to permit the alteration of evidence presented in the course of judicial or quasi-judicial proceedings. Amendments to these records are made through specific procedures established for the amendment of these records.

(i) Written notification will be provided to the requester within 10 working days of its receipt by the DeCA PA Officer. No notification will be provided to the requester if the action completed within the 10 days. Only under exceptional circumstances will more than 30 days be required to reach the decision to amend a request. If the decision is to grant all or in part of the request for amendment, the record will be amended and the requester informed and all other offices/personnel known to be keeping the information.

(ii) If the request for amendment is denied in whole or in part, The PA Officer will notify the individual in writing and provide the specific reasons and the procedures for appealing the decision.

(iii) All appeals are to be processed within 30 days. If additional time is required, the requester will be informed and provided when a final decision may be expected.

(e) *Fee assessments.* (1) DeCA personnel will only be charged the direct cost of copying and reproduction, computed using the appropriate portions of the fee schedule in DeCA Directive 30–12.[6] Normally, fees are waived automatically if the direct costs of a given request are less than $30. This fee waiver provision does not apply when a waiver has been granted to the individual before, and later requests appear to be an extension or duplication of that original request. Decisions to waive or reduce fees that exceed the automatic waiver threshold will be made on a case-by-case basis. Fees may not be charged when:

(i) Copying is performed for the convenience of the Government or is the only means to make the record available for the individual.

(ii) No reading room is available for the individual to review the record or a copy is made to keep the original in DeCA files.

(iii) The information may be obtained without charge under any other regulation, directive, or statute.

(2) No fees will be collected for search, retrieval, and review of records to determine releasability, copying of records when the individual has not requested a copy, transportation of records and personnel, or normal postage.

§ 327.8 Disclosure of personal information to other agencies and third parties

(a) *Disclosures and nonconsensual disclosures.* (1) All requests made by DeCA individuals for personal information about other individuals (third parties) will be processed under DeCA Directive 30–12[7] except when the third party personal information is contained in the Privacy record of the individual making the request.

(2) For the purposes of disclosure and disclosure accounting, the Department of Defense is considered a single agency.

(3) Personal information from DeCA systems of records will not be disclosed outside the DoD unless:

(i) The record has been requested by the individual to whom it pertains,

(ii) Written consent has been given by the individual to whom the record pertains for release to the requesting agency, activity, or individual, or

(iii) The release is pursuant to one of the specific nonconsensual purposes set forth in the Act.

(4) Records may be disclosed without the consent of a DeCA individual to any DoD official who has need for the record in the performance of their assigned duties. Rank, position, or title alone does not authorize this access. An official need for this information must exist.

(5) DeCA records must be disclosed if their release is required by 32 CFR part 285, which is implemented by DeCA Directive 30–12.[8] 32 CFR part 285 requires that records be made available to the public unless exempt from disclosure under the FOIA.

(b) *Normally releasable information.* Personal information that is normally releasable without the consent of a DeCA individual that does not imply a clearly unwarranted invasion of personal privacy:

(1) Civilian employees:

(i) Name,

(ii) Present and past position titles,

(iii) Present and past grades,

(iv) Present and past salaries,

(v) Present and past duty stations,

(vi) Office or duty telephone numbers,

(2) Military members:

(i) Full name,

(ii) Rank,

(iii) Date of rank,

(iv) Gross salary,

(v) Past duty assignments,

(vi) Present duty assignments,

(vii) Future assignments that are officially established,

[6] See footnote 3 to § 327.5.

[7] See footnote 3 to § 327.5.

[8] See footnote 3 to § 327.5.

(viii) Office or duty telephone numbers,

(ix) Source of commission,

(x) Promotion sequence number,

(xi) Awards and decorations,

(xii) Attendance at professional military schools,

(xiii) Duty status at any given time.

(3) All disclosures of personal information on civilian employees shall be made in accordance with the Office of Personnel Management (OPM) and all disclosures of personal information on military members shall be made in accordance with the standards established by 32 CFR part 285.

(4) The release of DeCA employees' home addresses and home telephone numbers is considered a clearly unwarranted invasion of personal privacy and is prohibited; however, these may be released without prior consent of the employee if:

(i) The employee has indicated previously that he or she consents to their release,

(ii) The releasing official was requested to release the information under the provisions of 32 CFR part 285.

(5) Before listing home addresses and home telephone numbers in any DeCA telephone directory, give the individuals the opportunity to refuse such a listing.

(c) *Disclosures for established routine uses.* (1) Records may be disclosed outside of DeCA without consent of the individual to whom they pertain for an established routine use.

(2) A routine use shall:

(i) Be compatible with the purpose for which the record was collected;

(ii) Indicate to whom the record may be released;

(iii) Indicate the uses to which the information may be put by the receiving agency; and

(iv) Have been published previously in the FEDERAL REGISTER.

(3) A routine use will be established for each user of the information outside DeCA who need official access to the records. This use may be discontinued or amended without the consent of the individual/s involved. Any routine use that is new or changed is published in the FEDERAL REGISTER 30 days before actually disclosing the record. In addition to routine uses established by DeCA individual system notices, blanket routine uses have been established. See Appendix C to this part.

(d) *Disclosure without consent.* DeCA records may be disclosed without the consent of the individual to whom they pertain to another agency within or under the control of the U.S. for a civil or criminal law enforcement activity if:

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

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

(3) 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.

(4) This disclosure provision applies when the law enforcement agency or instrumentality request the record, If the DoD Component discloses a record outside the DoD 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.

(e) *Disclosures to the public from health care records.* (1) The following general information may be released to the news media or public concerning a DeCA employee treated or hospitalized in DoD medical facilities and non-Federal facilities for whom the cost of the care is paid by DoD:

(i) Personal information concerning the patient that is provided in § 327.8 and under provisions of 32 CFR part 285.

(ii) The medical condition such as the date of admission or disposition and the present medical assessment of the individual's condition in the following terms if the medical doctor has volunteered the information:

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

(B) Whether the patient is conscious, semi-conscious or unconscious.

(2) Detailed medical and other personal information may be released on a DeCA employee only if the employee has given consent to the release. If the employee is not conscious or competent, no personal information, except that required by 32 CFR part 285, will be released until there has been enough improvement in the patient's condition for them to give informed consent.

(3) Any item of personal information may be released on a DeCA patient if the patient has given consent to its release.

(4) This part does not limit the disclosure of personal medical information for other government agencies' use in determining eligibility for special assistance or other benefits provided disclosure in pursuant to a routine use.

APPENDIX A TO PART 327—SAMPLE DECA RESPONSE LETTER

Mrs. Floria Employee
551 Florida Avenue
Oakland, CA 94618

Dear Mrs. Employee: This responds to your Privacy Act request dated (enter date of request), in which you requested (describe requested records).

Your request has been referred to our headquarters for further processing. They will respond directly to you. Any questions concerning your request may be made telephonically (enter Privacy Officer's telephone number) or in writing to the following address:

Defense Commissary Agency, Safety, Security, and Administration, Attention: FOIA/PA Officer, Fort Lee, VA 23801–1800.

I trust this information is responsive to your needs.

(Signature block)

APPENDIX B TO PART 327—INTERNAL MANAGEMENT CONTROL REVIEW CHECKLIST

(a) *Task:* Personnel and/or Organization Management.

(b) *Subtask:* Privacy Act (PA) Program.

(c) *Organization:*

(d) *Action officer:*

(e) *Reviewer:*

(f) *Date completed:*

(g) *Assessable unit:* The assessable units are HQ, DeCA, Regions, Central Distribution Centers, Field Operating Activities, and commissaries. Each test question is annotated to indicate which organization(s) is (are) responsible for responding to the question(s). Assessable unit managers responsible for completing this checklist are shown in the DeCA, MCP, DeCA Directive 70–2.[1]

(h) *Event cycle 1:* Establish and implement a Privacy Act Program.

(1) Risk: If prescribed policies, procedures and responsibilities of the Privacy Act Program are not adhered to, sensitive private information on individuals can be given out to individuals.

(2) Control Objectives: The prescribed policies, procedures and responsibilities contained in 5 U.S.C. 552a are followed to protect individual privacy and information release.

(3) Control Techniques: 32 CFR part 310 and DeCA Directive 30–13,[2] Privacy Act Program.

(i) Ensure that a PA program is established and implemented.

(ii) Appoint an individual with PA responsibilities and ensure the designation of appropriate staff to assist.

(4) Test Questions: Explain rationale for YES responses or provide cross-references where rationale can be found. For NO responses, cross-reference to where corrective action plans can be found. If response is NA, explain rationale.

(i) Is a PA program established and implemented in DeCA to encompass procedures for subordinate activities? (DeCA HQ/SA, Region IM). Response: Yes / No / NA. Remarks:

(ii) Is an individual appointed PA responsibilities? (DeCA HQ/SA, Region IM). Response: Yes / No / NA. Remarks:

(iii) Are the current names and office telephone numbers furnished OSD, Private Act Office of the PA Officer and the IDA? (DeCA HQ/SA). Response: Yes / No / NA. Remarks:

(iv) Is the annual PA report prepared and forwarded to OSD, Defense Privacy Office? (DeCA HQ/SA). Response: Yes / No / NA. Remarks:

(v) Is PA awareness training/orientation provided? Is in-depth training provided for personnel involved in the establishment, development, custody, maintenance and use of a system of records? (DeCA HQ/SA, Region). Response: Yes / No / NA. Remarks:

(vi) Is the PA Officer consulted by information systems developers for privacy requirements which need to be included as part of the life cycle management of information consideration in information systems design? (DeCA HQ/SA, Region). Response: Yes / No / NA. Remarks:

(vii) Is each system of records maintained by DeCA supported by a Privacy Act System Notice and has the systems notice been published in the FEDERAL REGISTER? (DeCA HQ/SA). Response: Yes / No / NA. Remarks:

---

[1] Copies may be obtained: Defense Commissary Agency, ATTN: FOIA/Privacy Officer, 1300 E. Avenue, Fort Lee, VA 23801–1800.

[2] See footnote 1 to this Appendix B.

(i) *Event cycle 2:* Processing PA Requests.

(1) Risk: Failure to process PA requests correctly could result in privacy information being released which subjects the Department of Defense, DeCA or individuals to criminal penalties.

(2) Control Objective: PA requests are processed correctly.

(3) Control Technique:

(i) Ensure PA requests are logged into a formal control system.

(ii) Ensure PA requests are answered promptly and correctly.

(iii) Ensure DeCA records are only withheld when they fall under the general and specific exemptions of 5 U.S.C. 552a and one or more of the nine exemptions under DeCA Directive 30–12,[3] Freedom of Information Act (FOIA) Program.

(iv) Ensure all requests are coordinated through the General Counsel.

(v) Ensure all requests are denied by the DeCA IDA.

(vi) Ensure all appeals are forwarded to the Director DeCA or his designee.

(4) Test Questions:

(i) Are PA requests logged into a formal control system? (DeCA HQ/SA, Region IM). Response: Yes / No / NA. Remarks:

(ii) Are individual requests for access acknowledged within 10 working days after receipt? (DeCA HQ/SA, Region IM). Response: Yes / No / NA. Remarks:

(iii) when more than 10 working days are required to respond to a PA request, is the requester informed, explaining the circumstances for the delay and provided an approximate date for completion? (DeCA HQ/SA, Region IM). Response: Yes / No / NA. Remarks:

(iv) Are DeCA records withheld only when they fall under one or more of the general or specific exemptions of the PA or one or more of the nine exemptions of the FOIA? (DeCA HQ/SA, Region IM). Response: Yes / No / NA. Remarks:

(v) Do denial letters contain the name and title or position of the official who made the determination, cite the exemption(s) on which the denial is based and advise the PA requester of their right to appeal the denial to the Director DeCA or designee? (DeCA HQ/SA). Response: Yes / No / NA. Remarks:

(vi) Are PA requests denied only by the HQ DeCA IDA? (All). Response: Yes/No/NA. Remarks:

(vii) Is coordination met with the General Counsel prior to forwarding a PA request to the IDA? (DeCA HQ/SA). Response: Yes/No/NA. Remarks:

(j) *Event cycle 3:* Requesting PA Information.

(1) Risk: Obtaining personal information resulting in a violation of the PA.

(2) Control Objective: Establish a system before data collection and storage to ensure no violation of the privacy of individuals.

(3) Control Technique: Ensure Privacy Act Statement to obtain personal information is furnished to individuals before data collection.

(4) Test Questions:

(i) Are all forms used to collect information about individuals which will be part of a system of records staffed with the PA Officer for correctness of the Privacy Act Statement? (DeCA HQ/SA, Region). Response: Yes/No/NA. Remarks:

(ii) Are Privacy Statements prepared and issued for all forms, formats and questionnaires that are subject to the PA, coordinated with the DeCA forms manager? (DeCA HQ/SA, Region). Response: Yes/No/NA. Remarks:

(iii) Do Privacy Act Statements furnished to individuals provide the following:

(A) The authority for the request.

(B) The principal purpose for which the information will be used.

(C) Any routine uses.

(D) The consequences of failing to provide the requested information. Yes/No/NA. Remarks:

(k) *Event cycle 4:* Records Maintenance.

(1) Risk: Unprotected records allowing individuals without a need to know access to privacy information.

(2) Control Objective: PA records are properly maintained throughout their life cycle.

(3) Control Technique: Ensure the prescribed policies and procedures are followed during the life cycle of information.

(4) Test Questions:

(i) Are file cabinets/containers that house PA records locked at all times to prevent unauthorized access? (All). Response: Yes/No/NA. Remarks:

(ii) Are personnel with job requirement (need to know) only allowed access to PA information? (All). Response: Yes/No/NA. Remarks:

(iii) Are privacy act records treated as unclassified records and designated 'For Official Use Only'? (All). Response: Yes/No/NA. Remarks:

(iv) Are computer printouts that contain privacy act information as well as disks, tapes and other media marked 'For Official Use Only'? (All). Response: Yes/No/NA. Remarks:

(v) Is a Systems Manager appointed for each automated/manual PA systems of records? (DeCA HQ/SA, Region). Response: Yes/No/NA. Remarks:

(vi) Are PA records maintained and disposed of in accordance with DeCA Directive

[3] See footnote 1 to this Appendix B.

30–2,[4] The Defense Commissary Agency Filing System? (All). Response: Yes/No/NA. Remarks:

(1) I attest that the above listed internal controls provide reasonable assurance that DeCA resources are adequately safeguarded. I am satisfied that if the above controls are fully operational, the internal controls for this sub-task throughout DeCA are adequate.

Safety, Security and Administration.

FUNCTIONAL PROPONENT.

I have reviewed this sub-task within my organization and have supplemented the prescribed internal control review checklist when warranted by unique environmental circumstances. The controls prescribed in this checklist, as amended, are in place and operational for my organization (except for the weaknesses described in the attached plan, which includes schedules for correcting the weaknesses).

ASSESSABLE UNIT MANAGER (Signature).

APPENDIX C TO PART 327–DECA BLANKET ROUTINE USES

(a) *Routine Use—Law Enforcement.* If a system of records maintained by a DoD Component, to carry out its functions, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, the agency concerned, whether Federal, State, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

(b) *Routine Use—Disclosure when Requesting Information.* A record from a system of records maintained by a Component may be disclosed as a routine use to a Federal, State, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a Component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

(c) *Routine Use—Disclosure of Requested Information.* A record from a system of records maintained by a Component may be disclosed to a Federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

(d) *Routine Use—Congressional Inquiries.* Disclosure from a system of records maintained by a Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

(e) *Routine Use—Private Relief Legislation.* Relevant information contained in all systems of records of the Department of Defense published on or before August 22, 1975, will be disclosed to the OMB in connection with the review of private relief legislation as set forth in OMB Circular A–19 at any stage of the legislative coordination and clearance process as set forth in that Circular.

(f) *Routine Use—Disclosures Required by International Agreements.* A record from a system of records maintained by a Component may be disclosed to foreign law enforcement, security, investigatory, or administrative authorities to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements including those regulating the stationing and status in foreign countries of DoD military and civilian personnel.

(g) *Routine Use—Disclosure to State and Local Taxing Authorities.* Any information normally contained in Internal Revenue Service (IRS) Form W–2 which is maintained in a record from a system of records maintained by a Component may be disclosed to State and local taxing authorities with which the Secretary of the Treasury has entered into agreements under 5 U.S.C., 5516, 5517, and 5520 and only to those State and local taxing authorities for which an employee or military member is or was subject to tax regardless of whether tax is or was withheld. This routine use is in accordance with Treasury Fiscal Requirements Manual Bulletin No. 76–07.

(h) *Routine Use—Disclosure to the Office of Personnel Management.* A record from a system of records subject to the Privacy Act and maintained by a Component may be disclosed to the Office of Personnel Management (OPM) concerning information on pay and leave, benefits, retirement deduction, and any other information necessary for the OPM to carry out its legally authorized government-wide personnel management functions and studies.

(i) *Routine Use—Disclosure to the Department of Justice for Litigation.* A record from a system of records maintained by this component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

[4] See footnote 2 to this Appendix B.

(j) *Routine Use—Disclosure to Military Banking Facilities Overseas.* Information as to current military addresses and assignments may be provided to military banking facilities who provide banking services overseas and who are reimbursed by the Government for certain checking and loan losses. For personnel separated, discharged, or retired from the Armed Forces, information as to last known residential or home of record address may be provided to the military banking facility upon certification by a banking facility officer that the facility has a returned or dishonored check negotiated by the individual or the individual has defaulted on a loan and that if restitution is not made by the individual, the U.S. Government will be liable for the losses the facility may incur.

(k) *Routine Use—Disclosure of Information to the General Services Administration (GSA).* A record from a system of records maintained by this component may be disclosed as a routine use to the General Services Administration (GSA) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

(l) *Routine Use—Disclosure of Information to the National Archives and Records Administration (NARA).* A record from a system of records maintained by this component may be disclosed as a routine use to the National Archives and Records Administration (NARA) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

(m) *Routine Use—Disclosure to the Merit Systems Protection Board.* A record from a system of records maintained by this component may be disclosed as a routine use to the Merit Systems Protection Board, including the Office of the Special Counsel for the purpose of litigation, including administrative proceedings, appeals, special studies of the civil service and other merit systems, review of OPM or component rules and regulations, investigation of alleged or possible prohibited personnel practices; including administrative proceedings involving any individual subject of a DoD investigation, and such other functions, promulgated in 5 U.S.C. 1205 and 1206, or as may be authorized by law.

(n) *Routine Use—Counterintelligence Purpose.* A record from a system of records maintained by this component may be disclosed as a routine use outside the DoD or the U.S. Government for the purpose of counterintelligence activities authorized by U.S. Law or Executive Order or for the purpose of enforcing laws which protect the national security of the United States.