DEFENSE LOGISTICS AGENCY
HEADQUARTERS
CAMERON STATION
ALEXANDRIA, VIRGINIA 22314

DLA-XA

DLA REGULATION
NO. 5400.21

26 Mar 85

PERSONAL PRIVACY AND RIGHTS OF INDIVIDUALS REGARDING THEIR PERSONAL RECORDS

(RCS DD-COMP(A) 1379)

(Supplementation is permitted by primary level field activities.)

I. PURPOSE AND SCOPE. This regulation implements the Privacy Act of 1974 (5 U.S.C. 552a) and DoD Directive 5400.11, Department of Defense Privacy Program. It applies to HQ DLA and all DLA field activities.

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

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

B. Collect personal information directly from the individuals to whom it pertains to the greatest extent practical.

C. Inform individuals who are asked to supply personal information for inclusion in any system of records:

1. The authority for the solicitation.
2. Whether furnishing the information is mandatory or voluntary.
3. The intended uses of the information.
4. The routine disclosures of the information that may be made outside DoD.
5. The effect on the individual of not providing all or any part of the requested information.

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

E. Make reasonable efforts to ensure that records containing personal information are accurate, relevant, timely, and complete for the purposes for which they are being maintained before making them available to any recipients outside DoD, other than a Federal agency, unless the disclosure is made under DLAR 5400.14, Availability to the Public of Official Information.

F. Keep no record that describes how individuals exercise their rights guaranteed by the First Amendment of 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.

G. Make reasonable efforts, when appropriate, to notify individuals whenever records pertaining to them are made available under compulsory legal process, if such process is a matter of public record.

H. 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.

This DLAR supersedes DLAR 5400.21, 15 Aug 75, and Change 1.

I. Establish rules of conduct for DoD personnel involved in the design, development, operation, or maintenance of any system of records and train them in these rules of conduct.

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

K. 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.

L. 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 DLAR 5400.14.
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.

M. Advise individuals on their rights to appeal any refusal to grant access to or amend any record pertaining to them, and to file a statement of disagreement with the record in the event amendment is refused.

III. 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 purpose of disclosing records subject to the Privacy Act among DoD Components, the Department of Defense is considered a single agency. For all other purposes including applications for access and amendment, denial of access or amendment, appeals from denials, and record keeping as regards release to non-DoD agencies, DLA 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 identity will be held in confidence or under an implied promise of such confidentiality if this implied promise was made before September 27, 1975.

D. Disclosure. The transfer of any personal information from a system of records by any means of communication 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.

E. 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.

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

G. Maintain. Includes maintain, collect, use, or disseminate.

H. Member of the Public. Any individual or party acting in a private capacity to include Federal employees or military personnel.

I. Official Use. Within the context of this DLAR, this term is used when officials and employees of a DLA activity have a demonstrated need for the use of any record or the information contained therein in the performance of their official duties.

J. 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.

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

L. 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.

(Continuation of III L)

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.

M. Records. Any item, collection, or grouping of information about an individual that is maintained by DLA, 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 the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

N. 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.

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

P. 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.

Q. System of Records. A group of records under the control of a DLA activity 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.

IV. SIGNIFICANT CHANGES. This DLAR has been completely revised and should be read in its entirety.

V. RESPONSIBILITIES

A. HQ DLA

1. The Chief, Resources Management Division, Office of Administration (DLA-XA) will:

a. Formulate policies, procedures, and standards necessary for uniform compliance with the Privacy Act by DLA activities.

b. Serve as the DLA Privacy Act Officer and DLA representative on the Defense Privacy Board.

c. Maintain a master registry of system notices published by DLA.

d. Develop or compile the rules, notices, and reports required under this regulation.

2. The General Counsel, DLA (DLA-G) will:

a. Serve as the appellate authority for denials of individual access and amendment of records.

b. Provide representation to the Defense Privacy Board Legal Committee.

c. Advise the Defense Privacy Office on the status of DLA privacy litigation.

3. The Command Security Officer, Office of Command Security, DLA (DLA-T) will formulate and implement protective standards for personal information maintained in automatic data processing systems and facilities.

B. The Heads of DLA Primary Level Field Activities (PLFAs) will:

1. Ensure that the collection, maintenance, use, or dissemination of record 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.

2. Designate a Privacy Act Officer to serve as the principal point of contact on privacy matters.

3. Ensure the internal operating procedures provide for effective compliance with the Privacy Act.

4. Establish a training program for those personnel whose duties involve responsibilities for systems of records affected by the Privacy Act.

VI. PROCEDURES

A. Individual Access

1. The access provisions of this DLAR are intended for use by individuals whose records are maintained in systems of records. Release of personal information to individuals under this DLAR is not considered public release of information.

2. Individuals will address requests for access to personal information about themselves in a system of records to the system manager or to the office designated in the system notice. Before being granted access to personal data, an individual may be required to provide reasonable verification of his or her identity. Identity verification procedures will be simple so as not to discourage individuals from seeking access to information about themselves; or be required of an individual seeking access to records which normally would be available under DLAR 5400.14.

a. Normally, when individuals seek personal access to records pertaining to themselves, identification is made from documents that normally are readily available, such as employee and military identification cards, driver's license, other licenses, permits, or passes used for routine identification purposes.

b. When access is requested by mail, identity verification may consist of the individual providing certain minimum identifying data, such as full name, date and place of birth, or such other personal information necessary to locate the record sought. If the information sought is sensitive, additional identifying data may be required. If notarization of requests is required, procedures will be established for an alternate method of verification for individuals who do not have access to notary services, such as military members overseas.

3. 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 a third party, the individual may be required to furnish a signed access authorization granting the third party access. An individual will not be refused access to his or her record solely for failure to divulge his or her social security number(SSN) unless it is the only method by which retrieval can be made. The individual is not required to explain or justify his or her need for access to any record under this DLAR.

4. Disclose medical records to the individual to whom they pertain, even if a minor, unless a judgment is made that access to such records could have an adverse effect on the mental or physical health of the individual. Normally, this determination will be made in consultation with a medical doctor. If it is determined that the release of the medical information may be harmful to the mental or physical health of the individual, send the record to a physician named by the individual and in the transmittal letter to the physician, explain why access by the individual without proper professional supervision could be harmful (unless it is obvious from the record). Do not require the physician to request the records for the individual. If the individual refuses or fails to designate a physician, the record will not be provided. Such refusal of access is not considered a denial for reporting purposes.

5. Requests by individuals for access to investigatory records pertaining to themselves and compiled for law enforcement purposes are processed under this DLAR or DLAR 5400.14 depending on which regulation gives them the greatest degree of access.

6. Certain documents under the physical control of DoD personnel and used to assist them in performing official functions, are not considered "agency records" within the meaning of this DLAR. Uncirculated personal notes and records that are not disseminated or circulated to any person or organization (for example, personal telephone lists or memory aids) that are retained or discarded at the author's discretion and over which DLA exercises no direct control, are not considered agency 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 DLAR.

7. Acknowledge requests for access within 10 working days after receipt and provide access within 30 working days.

B. Denial of Individual Access

1. Individuals may be formally denied access to a record pertaining to them only if the record was compiled in reasonable anticipation of civil action; is in a system of records that has been exempted from the access provisions of this DLAR under one of the permitted exemptions; contains classified information that has been exempted from the access provision of this DLAR under the blanket exemption for such material claimed for all DoD records systems; or is contained in a system of records for which access may be denied under some other Federal statute. Only deny the individual access to those portions of the records from which the denial of access serves some legitimate Governmental purpose.

2. An individual may be refused access if the record is not described well enough to enable it to be located with a reasonable amount of effort on the part of an employee familiar with the file; or access is sought by an individual who fails or refuses to comply with the established procedural requirements, including refusing to name a physician to receive medical records when required or to pay fees. Always explain to the individual the specific reason access has been refused and how he or she may obtain access.

3. Formal denials of access must be in writing and include as a minimum:

a. The name, title or position, and signature of the appropriate Head of the HQ DLA principal staff element or primary level field activity.

b. The date of the denial.

c. The specific reason for the denial, including specific citation to the appropriate sections of the Privacy Act or other statutes, this DLAR, or Code of Federal Regulations (CFR) authorizing the denial.

d. Notice to the individual of his or her right to appeal the denial within 60 calendar days.

e. The title or position and address of the Privacy Act appeals official, DLA-G, Cameron Station, Alexandria, VA 22304-6100.

4. The individual will file any appeals from denial of access within 60 calendar days of receipt of the denial notification. DLA-G will process all appeals within 30 days of receipt unless a fair and equitable review cannot be made within that period. The written appeal notification granting or denying access is the final DLA action on access.

5. The records in all systems of records maintained in accordance with the Office of Personnel Management (OPM) Government-wide system notices are technically only in the temporary custody of DLA. All requests for access to these records must be processed in accordance with the Federal Personnel Manual as well as this regulation. DLA-G is responsible for the appellate review of denial of access to such records.

C. Amendment of Records

1. Individuals are encouraged to review the personal information being maintained about them by DLA and to avail themselves of the procedures established by

this DLAR and other regulations to update their records. An individual may request the amendment of any record contained in a system of records pertaining to him or her unless the system of record has been exempted specifically from the amendment procedures of this DLAR. Normally, amendments under this DLAR are limited to correcting factual matters and not matters of official judgment, such as performance ratings, promotion potential, and job performance appraisals.

2. The applicant must adequately support his or her claim and may be required to provide identification to ensure that they are indeed seeking to amend a record pertaining to themselves and not, inadvertently or intentionally, the record of others. Consider the following factors when evaluating the sufficiency of a request to amend:

a. The accuracy of the information itself.

b. The relevancy, timeliness, completeness, and necessity of the recorded information for accomplishing an assigned mission or purpose.

3. Provide written acknowledgement of a request to amend within 10 working days of its receipt by the appropriate systems manager. There is no need to acknowledge a request if the action is completed within 10 working days and the individual is so informed. The letter of acknowledgement shall clearly identify the request and advise the individual when he or she may expect to be notified of the completed action. Only under the most exceptional circumstances will more than 30 days be required to reach a decision on a request to amend.

4. If the decision is made to grant all or part of the request for amendment, amend the record accordingly and notify the requester. Notify all previous recipients of the information, as reflected in the disclosure accounting records, that an amendment has been made and the substance of the amendment. Recipients who are known to be no longer retaining the information need not be advised of the amendment. All DoD Components and Federal agencies known to be retaining the record or information, even if not reflected in disclosure records, will be notified of the amendment. Advise the requester of these notifications, and honor all requests by the requester to notify specific Federal agencies of the amendment action.

5. If the request for amendment is denied in whole or in part, promptly advise the individual in writing of the decision to include:

a. The specific reason and authority for not amending.

b. Notification that he or she may seek further independent review of the decision by the Office of General Counsel, DLA (DLA-G).

6. Individual appeals of amendment denials must be submitted to the Office of General Counsel, DLA (DLA-G), Cameron Station, Alexandria, Virginia, 22304-6100 with all supporting materials. DLA-G will process all appeals within 30 days unless a fair review cannot be made within this time limit.

a. If the appeal is granted, DLA-G will promptly notify the requester and system manager of the decision. The system manager will amend the record(s) as directed and ensure that all prior known recipients of the records who are known to be retaining the record are notifed of the decision and the specific nature of the amendment and that the requester is notified as to which DoD Components and Federal agencies have been told of the amendment.

b. If the appeal is denied completely or in part, the individual is notified in writing by the reviewing official that:

(1) The appeal has been denied and the specific reason and authority for the denial.

(2) The individual may file a statement of disagreement with the appropriate authority and the procedures for filing this statement.

(3) If filed properly, the statement of disagreement shall be included in the records, furnished to all future recipients of the records, and provided to all prior recipients of the disputed records who are known to hold the record.

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

7. The records in all systems of records controlled by the Office of Personnel Management (OPM) Government-wide system notices are technically only temporarily in the custody of DLA. All requests for amendment of these records must be processed in accordance with the Federal Personnel Manual (FPM). A DLA denial authority may deny a request. However, the appeal process for all such denials must include a review by the Assistant Director for Agency Compliance and Evaluation, Office of Personnel Management, 1900 E Street, N.W., Washington, D.C. 20415. When an appeal is received from a DLA denial of amendment of the OPM controlled record, process the appeal in accordance with the FPM and notify the OPM appeal authority listed above. The individual may appeal any DLA decision not to amend the OPM records directly to OPM. OPM is the final review authority for any appeal from a denial to amend the OPM records.

8. If the reviewing authority refuses to amend the record as requested, the individual may submit a concise statement of disagreement setting forth his or her reasons for disagreeing with the decision not to amend.

a. If an individual chooses to file a statement of disagreement, annotate the record to indicate that the statement has been filed. Furnish copies of the statement of disagreement to all DoD Components and Federal agencies that have been provided copies of the disputed information and who may be maintaining the information.

b. When possible, incorporate the statement of disagreement into the record. If the statement cannot be made a part of the record, establish procedures to ensure that it is apparent from the records that a statement of disagreement has been filed and maintain the statement so that it can be obtained readily when the disputed information is used or disclosed. Automated record systems that are not programmed to accept statements of disagreement shall be annotated or coded so that they clearly indicate that a statement of disagreement is on file, and clearly identify the statement with the disputed information in the system. Provide a copy of the statement of disagreement whenever the disputed information is disclosed for any purpose.

9. A summary of reasons for refusing to amend may be included with any record for which a statement of disagreement is filed. Include in this summary only the reasons furnished to the individual for not amending the record. Do not include comments on the statement of disagreement. Normally, the summary and statement of disagreement are filed together. When disclosing information for which a summary has been filed, a copy of the summary may be included in the release, if desired.

D. Documentation. Establish a separate Privacy Case File to retain the documentation received and generated during the amendment or access process. There is no need to establish a Privacy Case File if the individual has not cited the Privacy Act or this DLAR. Privacy Case Files shall not be furnished or disclosed to anyone for use in making any determination about the individual other than determinations made under this DLAR. Only the items listed below may be included in the system of records challenged for amendment or for which access is sought. Do not retain copies of unamended records in the basic record system if the request for amendment is granted.

1. The following items relating to an amendment request may be included in the disputed record system:

a. Copies of the amended record.
b. Copies of the individual's statement of disagreement.
c. Copies of activity summaries.
d. Supporting documentation submitted by the individual.

(Continuation of VI D)

2. The following items relating to an access request may be included in the basic records system:

a. Copies of the request.

b. Copies of the activity action granting total access. (Note: A separate Privacy Case File need not be created in such cases.)

c. Copies of the activity action denying access.

d. Copies of any appeals filed.

e. Copies of the reply to the appeal.

E. Fees. An individual may be charged only for the direct cost of copying and reproduction, computed using the appropriate portions of the fee schedule in DLAR 5400.14, under the provisions of this regulation. 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. DLA activities may, however, set aside this automatic fee waiver provision when on the basis of good evidence it determines that the waiver of fees is not in the public interest. 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:

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

2. The record may be obtained without charge under any other regulation, directive, or statute.

3. Providing documents to members of Congress for copying records furnished even when the records are requested under the Privacy Act on behalf of a constituent.

F. Disclosures of Personal Information

1. For the purposes of disclosure and disclosure accounting, the Department of Defense is considered a single agency. Records pertaining to an individual may be disclosed without the consent of the individual to any DoD official who has need for the record in the performance of his or her assigned duties. Do not disclose personal information from a system of records outside the Department of Defense unless the record has been requested by the individual to whom it pertains; the written consent of the individual to whom the record pertains has been obtained for release of the record to the requesting agency, activity, or individual; or the release is for one of the specific nonconsensual purposes set forth in this regulation or DLAR 5400.14.

2. Except for releases made in accordance with DLAR 5400.14, before disclosing any personal information to any recipient outside DoD other than a Federal agency or the individual to whom it pertains:

a. Ensure that the records are accurate, timely, complete, and relevant for agency purposes.

b. Contact the individual, if reasonably available, to verify the accuracy, timeliness, completeness, and relevancy of the information, if this cannot be determined from the record.

c. If the information is not current and the individual is not reasonably available, advise the recipient that the information is believed accurate as of a specific date and any other known factors bearing on its accuracy and relevancy.

3. All records must be disclosed if their release is required by the Freedom of Information Act. DLAR 5400.14 requires that records be made available to the public unless exempted from disclosure by one of the nine exemptions found in the Freedom of Information Act. The standard for exempting most personal records, such as personnel records, medical records, and similar records, is found in DLAR 5400.14, paragraph IIIG6. Under the exemption, release of personal information can only be denied when its release would be a "clearly unwarranted invasion of personal privacy."

(Continuation of VI F 3)

a. All disclosures of personal information regarding Federal civilian employees will be made in accordance with the Federal Personnel Manual. Some examples of personal information regarding DoD civilian employees that normally may be released without a clearly unwarranted invasion of personal privacy include:

(1) Name.
(2) Present and past position titles.
(3) Present and past grades.
(4) Present and past salaries.
(5) Present and past duty stations.
(6) Office and duty telephone numbers.

b. All releases of personal information regarding military members shall be made in accordance with the standards established by DLAR 5400.14. While it is not possible to identify categorically information that must be released or withheld from military personnel records in every instance, the following items of personal information regarding military members normally may be disclosed without a clearly unwarranted invasion of their personal privacy:

(1) Full name.
(2) Rank.
(3) Date of rank.
(4) Gross salary.
(5) Past duty assignments.
(6) Present duty assignment.
(7) Future assignments that are officially established.
(8) Office or duty telephone numbers.
(9) Source of commission.
(10) Promotion sequence number.
(11) Awards and decorations.
(12) Attendance at professional military schools.
(13) Duty status at any given time.

c. All releases of personal information regarding civilian personnel not subject to the FPM shall be made in accordance with the standards established by DLAR 5400.14. While it is not possible to identify categorically those items of personal information that must be released regarding civilian employees not subject to the FPM, such as nonappropriated fund employees, normally the following items may be released without a clearly unwarranted invasion of personal privacy:

(1) Full name.
(2) Grade or position.
(3) Date of grade.
(4) Gross salary.
(5) Present and past assignments.
(6) Future assignments, if officially established.
(7) Office or duty telephone numbers.

4. A request for a home address or telephone number may be referred to the last known address of the individual for a direct reply by him or her to the requester. In such cases the requester will be notified of the referral. The release of home addresses and home telephone numbers normally is considered a clearly unwarranted invasion of personal privacy and is prohibited. However, these may be released without prior specific consent of the individual if:

a. The individual has indicated previously that he or she has no objection to their release.

b. The source of the information to be released is a public document such as commercial telephone directory or other public listing.

c. The release is required by Federal statute (for example, pursuant to Federally-funded state programs to locate parents who have defaulted on child support payments (42 U.S.C. Section 653)).

d. The releasing official releases the information under the provisions of DLAR 5400.14.

5. Records may be disclosed outside DoD without consent of the individual to whom they pertain for an established routine use. Routine uses may be established, discontinued, or amended without the consent of the individuals involved. However, new or changed routine uses must be published in the Federal Register at least 30 days before actually disclosing any records under their provisions. In addition to the routine uses established by the individual system notices, common blanket routine uses for all DLA-maintained systems of records have been established. These blanket routine uses are published in DLAH 5400.1, DLA Systems of Records Handbook. Unless a system notice specifically excludes a system from a given blanket routine use, all blanket routine uses apply.

6. Records in DLA systems of records may be disclosed without the consent of the individuals to whom they pertain to the Bureau of the Census for purposes of planning or carrying out a census survey or related activities.

7. Records may be disclosed for statistical research and reporting without the consent of the individuals to whom they pertain. Before such disclosures, the recipient must provide advance written assurance that the records will be used as statistical research or reporting records; the records will only be transferred in a form that is not individually identifiable; and the records will not be used, in whole or in part, to make any determination about the rights, benefits, or entitlements of specific individuals. A disclosure accounting is not required.

8. Records may be disclosed without the consent of the individual to whom they pertain to the National Archives Records Service (NARS) if they have historical or other value to warrant continued preservation; or for evaluation by NARS to determine if a record has such historical or other value. Records transferred to a Federal Record Center (FRC) for safekeeping and storage do not fall within this category. These remain under the control of the transferring activity, and the FRC personnel are considered agents of the activity which retain control over the records. No disclosure accounting is required for the transfer of records to FRCs.

9. Records may be disclosed without the consent of the individual to whom they pertain 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, provided the civil or criminal law enforcement activity is authorized by law; the head of the law enforcement activity or a designee has made a written request specifying the particular records desired and the law enforcement purpose (such as criminal investigations, enforcement of civil law, or a similar purpose) for which the record is sought; and there is no Federal statute that prohibits the disclosure of the records. Normally, blanket requests for access to any and all records pertaining to an individual are not honored. When a record is released to a law enforcement activity, maintain a disclosure accounting. This disclosure accounting will not be made available to the individual to whom the record pertains if the law enforcement activity requests that the disclosure not be released.

10. Records may be disclosed without the consent of the individual to whom they pertain if disclosure is made under compelling circumstances affecting the health or safety of any individual. The affected individual need not be the subject of the

record disclosed. When such a disclosure is made, notify the individual who is the subject of the record. Notification sent to the last known address of the individual as reflected in the records is sufficient.

11. Records may be disclosed without the consent of the individual to whom they pertain to either House of the Congress or to any committee, joint committee or subcommittee of Congress if the release pertains to a matter within the jurisdiction of the committee. Records may also be disclosed to the General Accounting Office (GAO) in the course of the activities of GAO.

12. Records may be disclosed without the consent of the person to whom they pertain under a court order signed by a judge of a court of competent jurisdiction. Releases may also be made under the compulsory legal process of Federal or state bodies having authority to issue such process.

a. When a record is disclosed under this provision, make reasonable efforts to notify the individual to whom the record pertains, if the legal process is a matter of public record.

b. If the process is not a matter of public record at the time it is issued, seek to be advised when the process is made public and make reasonable efforts to notify the individual at that time.

c. Notification sent to the last known address of the individual as reflected in the records is considered reasonable effort to notify. Make a disclosure accounting each time a record is disclosed under a court order or compulsory legal process.

13. Certain personal information may be disclosed to consumer reporting agencies as defined by the Federal Claims Collection Act. Information which may be disclosed to a consumer reporting agency includes:

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

b. The amount, status, and history of the claim.

c. The agency or program under which the claim arose.

G. Disclosure Accounting

1. Keep an accurate record of all disclosures made from any system of records except disclosures to DoD personnel for use in the performance of their official duties or under DLAR 5400.14. In all other cases a disclosure accounting is required even if the individual has consented to the disclosure of the information pertaining to him or her.

2. Use any system of disclosure accounting that will provide the necessary disclosure information. As a minimum, disclosure accounting will contain the date of the disclosure, a description of the information released, the purpose of the disclosure, the name and address of the person or agency to whom the disclosure was made. When numerous similar records are released (such as transmittal of payroll checks to a bank), identify the category of records disclosed and include the data required in some form that can be used to construct an accounting disclosure record for individual records if required. Retain disclosure accounting records for 5 years after the disclosure or the life of the record, whichever is longer.

3. Make available to the individual to whom the record pertains all disclosure accountings except when the disclosure has been made to a law enforcement activity and the law enforcement activity has requested that disclosure not be made, or the system of records has been exempted from the requirement to furnish the disclosure accounting. If disclosure accountings are not maintained with the record and the individual requests access to the accounting, prepare a listing of all disclosures and provide this to the individual upon request.

(Continuation of VI)

H. Collecting Personal Information

1. Collect to the greatest extent practicable 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.

2. When an 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 (forms, personal interviews, stylized formats, telephonic interviews, or other methods). The statement enables the individual to make an informed decision whether to provide the information requested. If the personal information solicited is not to be incorporated into a system of records, the statement need not be given. The Privacy Act Statement shall be concise, current, and easily understood. It must include:

a. The specific Federal statute or Executive Order that authorizes collection of the requested information.

b. The principal purpose or purposes for which the information is to be used.

c. The routine uses that will be made of the information.

d. Whether providing the information is voluntary or mandatory.

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

3. The Privacy Act Statement may appear as a public notice (sign or poster), conspicuously displayed in the area where the information is collected, such as at check-cashing facilities or identification photograph facilities. The individual normally is not required to sign the Privacy Act Statement. Provide the individual a written copy of the Privacy Act Statement upon request. This must be done regardless of the method chosen to furnish the initial advisement.

4. Include in the Privacy Act Statement specifically whether furnishing the requested personal data is mandatory or voluntary. A requirement to furnish personal data is mandatory only when a Federal statute, Executive Order, regulation, or other lawful order specifically imposes a duty on the individual to provide the information sought, and the individual is subject to a penalty if he or she fails to provide the requested information. If providing the information is only a condition of a prerequisite to granting a benefit or privilege and the individual has the option of requesting the benefit or privilege, providing the information is always voluntary. However, the loss or denial of the privilege, benefit, or entitlement sought may be listed as a consequence of not furnishing the requested information.

5. It is unlawful for any Federal, state, or local government agency to deny an individual any right, benefit, or privilege provided by law because the individual refuses to provide his or her SSN. However, if a Federal statute requires that the SSN be furnished or if the SSN is required to verify the identity of the individual in a system of records that was established and in use before January 1, 1975, and the SSN was required as an identifier by a statute or regulation adopted before that date, this restriction does not apply.

a. When an individual is requested to provide his or her SSN, he or she must be told:

(1) The uses that will be made of the SSN.

(2) The statute, regulation, or rule authorizing the solicitation of the SSN.

(3) Whether providing the SSN is voluntary or mandatory.

b. Include in any systems notice for any system of records that contains SSNs a statement indicating the authority for maintaining the SSN and the source of the SSNs in the system. If the SSN is obtained directly from the individual indicate whether this is voluntary or mandatory.

c. Upon entrance into Military Service or civilian employment with DoD, individuals are asked to provide their SSNs. The SSN becomes the service or employment number for the individual and is used to establish personnel, financial, medical, and other official records. After an individual has provided his or her SSN for the purpose of establishing a record, a Privacy Act Statement 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. However, if the SSN is to be written down and retained for any purpose by the requesting official, the individual must be provided a Privacy Act Statement.

6. DLAR 7760.1, Forms Management Program, provides guidance on administrative requirements for Privacy Act Statments used with DLA forms. Forms subject to the Privacy Act issued by other Federal agencies have a Privacy Act Statement attached or included. Always ensure that the statement prepared by the originating agency is adequate for the purpose for which the form will be used by the DoD activity. If the Privacy Act Statement provided is inadequate, the activity concerned will prepare a new statement or a supplement to the existing statement before using the form. Forms issued by agencies not subject to the Privacy Act (state, municipal, and other local agencies) do not contain Privacy Act Statements. Before using a form prepared by such agencies to collect personal data subject to this DLAR, an appropriate Privacy Act Statement must be added.

I. Systems of Records

1. To be subject to this regulation, a "system of records" must consist of records retrieved by the name of an individual or some other personal identifier and be under the control of a DLA activity. Records in a group of records that may be retrieved by a name or personal identifier are not covered by this DLAR. The records must be, in fact, retrieved by name or other personal identifier to become a system of records for the purpose of this DLAR.

2. Retain in a system of records only that personal information which is relevant and necessary to accomplish a purpose required by a Federal statute or an Executive Order. The existence of a statute or Executive Order mandating that maintenance of a system of records does not abrogate the responsibility to ensure that the information in the system of records is relevant and necessary.

3. Do not maintain any records describing how an individual exercises his or her rights guaranteed by the First Amendment of the U.S. Constitution unless expressly authorized by Federal statute or the individual. 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.

4. Maintain all personal information used to make any determination about an individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual in making any such determination. Before disseminating any personal information from a system of records to any person outside DoD, other than a Federal agency, make reasonable efforts to ensure that the information to be disclosed is accurate, relevant, timely, and complete for the purpose it is being maintained.

5. Establish appropriate administrative, technical and physical safeguards to ensure that the records in every system of records are protected from unauthorized alteration or disclosure and that their confidentiality is protected. Protect the records against reasonably anticipated threats or hazards. Tailor safeguards specifically to the vulnerabilities of the system and the type of records in the system, the sensitivity of the personal information stored, the storage medium used and, to a degree, the number of records maintained.

a. Treat all unclassified records that contain personal information that normally would be withheld from the public as if they were designated "For Official Use Only" and safeguard them in accordance with the standards established by DLAR 5400.14 even if they are not marked "For Official Use Only."

b. Special administrative, physical, and technical procedures are required to protect data that are stored or being processed temporarily in an automated data processing (ADP) system or in a word processing activity to protect it against threats unique to those environments (see DLAM 5200.1, ADP Security Manual, and enclosure 4 of this regulation).

6. Dispose of records containing personal data so as to prevent inadvertent compromise. Disposal methods such as tearing, burning, melting, chemical decomposition, pulping, pulverizing, shredding, or mutilation are considered adequate if the personal data is rendered unrecognizable or beyond reconstruction.

a. The transfer of large quantities of records containing personal data (for example, computer cards and printouts) in bulk to a disposal activity, such as the Defense Property Disposal Office, is not a release of personal information under this DLAR. The sheer volume of such transfers makes it difficult or impossible to identify readily specific individual records.

b. When disposing of or destroying large quantities of records containing personal information, care must be exercised to ensure that the bulk of the records is maintained so as to prevent specific records from being readily identified. If bulk is maintained, no special procedures are required.

7. When DLA 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 of the record system affected are considered to be maintained by DLA and are subject to this DLAR. The activity concerned is responsible for applying the requirements of this DLAR to the contractor. The contractor and its employees are to be considered employees of DLA for purposes of the sanction provisions of the Privacy Act during the performance of the contract. See the Federal Acquisition Regulation (FAR), section 24.000.

J. System Notices

1. A notice of the existence of each system of records must be published in the Federal Register. While system notices are not subject to formal rulemaking procedures, advance public notice must be given before an activity may begin to collect personal information or use a new system of records. The notice procedures require that:

a. The system notice describes the contents of the record system and the routine uses for which the information in the system may be released.

b. The public be given 30 days to comment on any proposed routine uses before implementation.

c. The notice contains the date on which the system will become effective.

2. Enclosure 1 of this regulation discusses the specific elements required in a system notice. DLAH 5400.1 contains systems notices published by DLA.

3. In addition to system notices, reports are required for new and altered systems of records. The criteria of these reports are outlined in enclosures 2 and 3 of this regulation. No report is required for amendments to existing systems which do not meet the criteria for altered record systems.

4. System managers 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:

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

(Continuation of VI J 4)

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

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

d. The length of time each item of personal information must be retained.

e. The cost of maintaining the information.

f. The necessity and relevancy of the information to the purpose for which it was collected.

5. Systems notices and reports of new and altered systems will be submitted to DLA-XA as required.

K. Exemptions. The Director, DLA will designate the DLA records which are to be exempted from certain provisions of the Privacy Act. DLA-XA will publish in the Federal Register information specifying the name of each designated system, the specific provisions of the Privacy Act from which each system is to be exempted, the reasons for each exemption, and the reason for each exemption of the record system.

1. General Exemptions. To qualify for a general exemption, as defined in the Privacy Act, the system of records must be maintained by a system manager who performs as his/her principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities. Such system of records must consist of:

a. Information compiled for the purpose of identifying individual criminal offenders and alleged offenders and containing only identifying data and notations or arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole, and probation status.

b. Information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual.

c. Reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

2. Specific Exemption. To qualify for a specific exemption, as defined by the Privacy Act, the systems of records must be:

a. Specifically authorized under criteria established by an Executive Order to be kept classifed in the interest of national defense or foreign policy and are in fact properly classified pursuant to such Executive Order.

b. Investigatory material compiled for law enforcement purposes other than material covered under a general exemption. However, an individual will not be denied access to information which has been used to deny him/her a right or privilege unless disclosure would reveal a source who furnished information to the Government under a promise that the identity of the source would be held in confidence. For investigations made after 27 Sep 75, the identity of the source may be treated as confidential only if based on the expressed guarantee that the identity would not be revealed.

c. Maintained in connection with providing protective services to the President of the United States or other individuals protected pursuant to 18 U.S.C. 3056.

d. Used only to generate aggregate statistical data or for other similarly evaluative or analytic purposes, and which are not used to make decisions on the rights, benefits, or entitlements of individuals except for the disclosure of a census record permitted by 13 U.S.C. 8.

e. 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 that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the source would be held in confidence, or prior to 27 Sep 75, under an implied promise that the identity of the source would be held in confidence.

f. Testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service, the disclosure of which would compromise the objectivity or fairness of the testing or elimination process.

g. Evaluation material used to determine potential for promotion in the Military Services, but only the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence or prior to 27 Sep 75, under an implied promise that the identity of the source would be held in confidence. System managers will specify those categories of individuals for whom pledges of confidentiality may be made when obtaining information on an individual's suitability for promotion.

h. Exemption rules for DLA systems of records are published in enclosure 8 of this regulation.

L. Matching Program Procedures. The OMB has issued special guidelines to be followed in programs that match the personal records in the computerized data bases of two or more Federal agencies by computer (see enclosure 5). These guidelines are intended to strike a balance between the interest of the Government in maintaining the integrity of Federal programs and the need to protect individual privacy expectations. They do not authorize matching programs as such and each matching program must be justified individually in accordance with the OMB guidelines.

1. Forward all requests for matching programs to include necessary routine use amendments and analysis and proposed matching program reports to DLA-XA. Changes to existing matching programs shall be processed in the same manner as a new matching program report.

2. No time limits are set by the OMB guidelines. However, in order to establish a new routine use for a matching program, the amended system notice must have been published in the Federal Register at least 30 days before implementation. Submit the documentation required above to DLA-XA at least 60 days before the proposed initiation date of the matching program. Waivers to the 60 days' deadline may be granted for good cause shown. Requests for waivers will be in writing and fully justified.

3. For the purpose of the OMB guidelines, DoD and all DoD Components are considered a single agency. Before initiating a matching program using only the records of two or more DoD activities, notify DLA-XA that the match is to occur. Further information may be requested from the activity proposing the match.

4. System managers shall review annually each system of records to determine if records from the system are being used in matching programs and whether the OMB Guidelines have been complied with.

VII. FORMS AND REPORTS. DLA activities may be required to provide data under reporting requirements established by the Defense Privacy Office and DLA-XA. Any report established shall be assigned Report Control Symbol DD-COMP(A) 1379.

BY ORDER OF THE DIRECTOR

GEORGE A. WHITE
Colonel, USAF
for Staff Director, Administration

8 Encl
1. Instructions for Preparation of System Notices
2. Criteria for New and Altered Record Systems
3. Instructions for Preparation of Reports to New or Altered Systems
4. Word Processing Center (WPC) Safeguards
5. OMB Guidelines for Matching Programs
6. Litigation Status Sheet
7. Privacy Act Enforcement Actions
8. DLA Exemption Rules

DISTRIBUTION
2

COORDINATION: DLA-T, DLA-C, DLA-G, DLA-Z, DLA-Y, DLA-K, DLA-KS, DLA-LP, DLA-LR

INSTRUCTIONS FOR PREPARATION OF SYSTEM NOTICES

A. System identification. See DLAH 5400.1.

B. System name. The name of the system reasonably identifies the general purpose of the system and, if possible, the general categories of individuals involved. Use acronyms only parenthetically following the title or any portion thereof, such as, "Joint Uniform Military Pay System (JUMPS)." Do not use acronyms that are not commonly known unless they are preceded by an explanation. The system name may not exceed 55 character positions including punctuation and spacing.

C. System location

1. For systems maintained in a single location provide the exact office name, organizational identity, and address or routing symbol. For geographically or organizationally decentralized systems, specify each level of organization or element that maintains a segment of the system. For automated data systems with a central computer facility and input/output terminals at several geographically separated locations, list each location by category.

2. When multiple locations are identified by type of organization, the system location may indicate that official mailing addresses are contained in an address directory published as an appendix to DLAH 5400.1. DLA-XA will obtain information concerning format requirements for preparation of an address directory from the 1st Information Systems Group (1ISG), Room 3A-1066, The Pentagon, Washington, D.C. 20330-6345.

3. If no address directory is used or the addresses in the directory are incomplete, the address of each location where a segment of the record system is maintained must appear under the "System Location" caption. Classified addresses are not listed, but the fact that they are classified is indicated. Use the standard U.S. Postal Service two letter state abbreviation symbols and zip codes for all domestic addresses.

D. Categories of individuals covered by the system. Set forth the specific categories of individuals to whom records in the system pertain in clear, easily understood, nontechnical terms. Avoid the use of broad over-general descriptions, such as "all DLA personnel" or "all civilian personnel" unless this actually reflects the category of individuals involved.

E. Categories of records in the system. Describe in clear, nontechnical terms the types of records maintained in the system. Only documents actually retained in the system of records will be described, not source documents that are used only to collect data and then destroyed.

F. Authority for maintenance of the system

1. Cite the specific provisions of the Federal statute or Executive Order that authorizes the maintenance of the system. Include with citations for statutes the popular names, when appropriate (for example, Title 51, United States Code, Section

2103, "Tea-Tasters Licensing Act"), and for Executive Orders, the official title (for example, Executive Order No. 9397, "Numbering System for Federal Accounts Relative to Individual Persons").

2. For administrative housekeeping records, cite the directive establishing DLA as well as the Secretary of Defense authority to issue the directive. For example, "Pursuant to the authority contained in the National Security Act of 1947, as amended (10 U.S.C. 133d), the Secretary of Defense has issued DoD Directive 5105.22, Defense Logistics Agency (DLA), the charter of the Defense Logistics Agency (DLA) as a separate Agency of the Department of Defense under his control. Therein, the Director, DLA, is charged with the responsibility of maintaining all necessary and appropriate records."

G. Purpose or Purposes. List the specific purposes for maintaining the system of records by the activity. Include the uses made of the information within DLA and the Department of Defense (so-called "internal routine uses").

H. Routine uses

1. The blanket routine uses that appear in DLAH 5400.1 apply to all systems notices unless the individual system notice specifically states that one or mone of them do not apply to the system. For all other routine uses, when practical, list the specific activity to which the record may be released, to include any routine automated system interface (for example, "to the Department of Justice, Civil Rights Compliance Division," "to the Veterans Administration, Office of Disability Benefits," or "to state and local health agencies").

2. For each routine use identified, include a statement as to the purpose or purposes for which the record is to be released to the activity. Do not use general statements, such as, "to other Federal agencies as required" and "to any other appropriate Federal agency."

I. Policies and practices for storing, retiring, accessing, retaining, and disposing of records. This caption is subdivided into four parts:

1. Storage. Indicate the medium in which the records are maintained. (For example, a system may be "automated, maintained on magnetic tapes or disks," "manual, maintained in paper files," or "hybrid, maintained in a combination of paper and automated form.") Storage does not refer to the container or facility in which the records are kept.

2. Retrievability. Specify how the records are retrieved (for example, name and SSN, name, SSN) and indicate whether a manual or computerized index is required to retrieve individual records.

3. Safeguards. List the categories of DLA personnel having immediate access and those responsible for safeguards (such as storage in safes, vaults, locked cabinets or rooms, use of guards, visitor registers, personnel screening, or computer "fail-safe" systems software). Do not describe safeguards in such detail as to compromise system security.

4. Retention and Disposal. Indicate how long the record is retained. When appropriate, state the length of time the records are maintained by the activity, when they are transferred to a Federal Records Center, length of retention at the Records Center and when they are transferred to the National Archives or are destroyed. A reference to DLAM 5015.1, Files Maintenance and Disposition, or other issuances without further detailed information is insufficient.

J. System manager or managers and address

1. List the title and address of the official responsible for the management of the system. If the title of the specific official is unknown, such as for a local system, specify the local commander or office head as the systems manager.

2. For geographically separated or organizationally decentralized activities for which individuals may deal directly with officials at each location in exercising their rights, list the position or duty title of each category of officials responsible for the system or a segment thereof.

3. Do not include business or duty addresses if they are listed in DLAH 5400.1.

K. Notification procedures

1. If the record system has been exempted from subsection (e)(4)(G) of the Privacy Act, so indicate.

2. For all nonexempt systems, describe how an individual may determine if there are records pertaining to him or her in the system. The procedural rules may be cited, but include a brief procedural description of the needed data. Provide sufficient information in the notice to allow an individual to exercise his or her rights without referrals to this regulation.

3. As a minimum, the caption will include:

a. The official title (normally the system manager) and official address to which request is to be directed.

b. The specific information required to determine if there is a record of the individual in the system.

c. Identification of the offices through which the individual may obtain access.

d. A description of any proof of identity required.

4. When appropriate, the individual may be referred to an activity official who shall provide this data to him or her.

L. Record access procedures

1. If the record system has been exempted from subsection (e)(4)(H) of the Privacy Act, so indicate.

2. For all nonexempt record systems, describe the procedures under which individuals may obtain access to the record pertaining to them in the system. When appropriate, the individual may be referred to the system manager or activity official to obtain access procedures. Do not repeat the addresses listed in DLAH 5400.1, but refer the individual to that directory.

M. Contesting record procedures

1. If the record system has been exempted from subsection (e)(4)(H) of the Privacy Act, so indicate.

2. For all nonexempt systems of records, state briefly how an individual may contest the content of a record pertaining to him or her in the system. The detailed procedures for contesting record accuracy, refusal of access or amendment, or initial review and appeal need not be included if they are readily available elsewhere and can be referred to by the public. (For example, "The Defense Logistics Agency rules for contesting contents and for appealing initial determinations are contained in DLAR 5400.21 (32 CFR Part 1286).")

3. The individual may also be referred to the system manager to determine these procedures.

N. Record source categories

1. If the record system has been exempted from subsection (e)(4)(I) of the Privacy Act, so indicate.

2. For all nonexempt systems of records, list the sources of the information in the system. Specific individuals or institutions need not be identified by name, particularly if these sources have been granted confidentiality.

O. System exempted from certain provisions of the Privacy Act

1. If no exemption has been claimed for the system, indicate "None."

2. If there is an exemption claimed, indicate specifically under which subsection of the Privacy Act it is claimed. Cite the regulation and CFR section containing the exemption rule for the system. (For example, "Parts of this record system may be exempt under Title 5, United States Code, Sections 552a(k)(2) and (5), as applicable. See exemption rules contained in DLAR 5400.21 (32 CFR Part 1286).")

CRITERIA FOR NEW AND ALTERED RECORD SYSTEMS

A. Criteria for a new record system. A new system of records is one for which there has been no system notice published in the Federal Register. If a notice for a system of records has been canceled or deleted, before reinstating or reusing 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 whenever one of the following actions occurs or is proposed:

1. A significant increase or change in the number or type of individuals about whom records are maintained.

a. Only changes that alter significantly the character and purpose of the records system are considered alterations.

b. Increases in numbers of individuals due to normal growth are not considered alterations unless they truly alter the character and purpose of the system.

c. Increases that change significantly the scope of population covered (for example, expansion of a system of records covering a single PLFA's enlisted personnel to include all of DLA enlisted personnel would be considered an alteration).

d. A reduction in the number of individuals covered is not an alteration, but only an amendment.

e. All changes that add new categories of individuals to system coverage require a change to the "Categories of individuals covered by the system" caption of the notice and may require changes to the "Purpose(s)" caption.

2. An expansion in the types or categories of information maintained.

a. The addition of any new category of records not described under the "Categories of Records in System" caption is considered an alteration.

b. Adding a new data element which is clearly within the scope of the categories of records described in the existing notice is an amendment.

c. All changes under this criterion require a change to the "Categories of Records in System" caption of the notice.

3. An alteration in the manner in which the records are organized or the manner in which the records are indexed and retrieved.

a. The change must alter the nature of use or scope of the records involved (for example, combining records systems in a reorganization).

INSTRUCTIONS FOR PREPARATION OF REPORTS TO NEW OR ALTERED SYSTEMS

The report on a new or altered system will consist of a transmittal letter, a narrative statement, and include supporting documentation.

A. Transmittal Letter. The transmittal letter shall include any request for waivers. The narrative statement will be attached.

B. Narrative Statement. The narrative statement is typed in double space on standard bond paper. The statement includes:

1. System identification and name. This caption sets forth the identification and name of the system.

2. Responsible official. The name, title, address, and telephone number of the official responsible for the report and to whom inquiries and comments about the report may be directed by Congress, the Office of Management and Budget, or Defense Privacy Office.

3. Purpose of the system or nature of the change proposed. Describe the purpose of the new system. For an altered system, describe the nature of the change being proposed.

4. Authority for the system. See enclosure 1 of this regulation.

5. Number of individuals. The approximate number of individuals about whom records are to be maintained.

6. Information on First Amendment activities. Describe any information to be kept on the exercise of the individual's First Amendment rights and the basis for maintaining it.

7. Measures to ensure information accuracy. If the system is to be used to make determinations about the rights, benefits, or entitlements of individuals, describe the measures being established to ensure the accuracy, currency, relevance, and completeness of the information used for these purposes.

8. Other measures to ensure system security. Describe the steps taken to minimize the risk of unauthorized access to the system. A more detailed assessment of security risks and specific administrative, technical, and physical safeguards will be available for review upon request.

9. Relationship to state and local government activities. Describe the relationship of the system to state or local government activities that are the sources, recipients, or users of the information in the system.

C. Supporting Documentation. Item 10 of the narrative is captioned Supporting Documents. A positive statement for this caption is essential for those enclosures that are not required to be enclosed. For example, "No changes to the existing DLA procedural or exemption rules (32 CFR Part 1286) are required for this proposed system." List in numerical sequence only those enclosures that are actually furnished. The following are typical enclosures that may be required:

1. For a new system, an advance copy of the system notice which is proposed for publication; for an altered system an advance copy of the notice reflecting the specific changes proposed.

2. An advance copy of any proposed exemption rule if the new or altered system is to be exempted. If there is no exemption, so state in the narrative.

3. Any other supporting documentation that may be pertinent or helpful in understanding the need for the system or clarifying its intended use. While not required, such documentation, when available, is helpful in evaluating the new or altered system.

WORD PROCESSING CENTER (WPC) SAFEGUARDS

A. MINIMUM STANDARDS OF PROTECTION. All personal data processed using word processing equipment will be afforded the standards of protection required by this regulation. The special considerations discussed in this enclosure are primarily for Word Processing Centers (WPCs) operating independent of the customer's function. However, managers of word processing systems are encouraged to consider and adopt, when appropriate, the special considerations described. WPCs that are not independent of a customer's function are not required to prepare formal written risk assessments.

B. WPC INFORMATION FLOW. In analyzing procedures required to safeguard adequately personal information in a WPC, the basic elements of WPC information flow and control must be considered. These are: information receipt, information processing, information return, information storage and filing. WPCs do not control information acquisition or its ultimate use by the customers and, therefore, these are not addressed.

C. SAFEGUARDING INFORMATION DURING RECEIPT

1. The word processing manager will establish procedures:

a. That require each customer who requests that information subject to this DLAR be processed to identify specifically that information to the WPC personnel. This may be done by:

(1) Providing a check-off type entry on the WPC work requests.

(2) Requiring that the WPC work requests be stamped with a special legend, or that a special notation be made on the work requests.

(3) Predesignating specifically a class of documents as coming within the provisions of this DLAR (such as, all officer effectiveness reports, all recall rosters, and all medical protocols).

(4) Using a special cover sheet both to alert the WPC personnel as to the type information, and to protect the document during transmittal.

(5) Requiring an oral warning on all dictation.

(6) Any other procedures that ensure the WPC personnel are alerted to the fact that personal data subject to this DLAR is to be processed.

b. To ensure that the operators or other WPC personnel who receive data for processing not identified as being under the provisions of this DLAR, but that appear to be personal, promptly call the information to the attention of the WPC supervisor or the customer.

c. To ensure that any request for the processing of personal data which the customer has not identified as being in a system of record, and that appears to meet the criteria set forth in this regulation, is called to the attention of the appropriate supervisory personnel and system manager.

2. The WPC supervisor will ensure that personal information is not inadvertently compromised within the WPC.

D. SAFEGUARDING INFORMATION DURING PROCESSING

1. Each WPC supervisor will establish internal safeguards that will protect personal data from compromise while it is being processed.

2. Physical safeguards may include:

a. Controls on individual access to the center.

b. Machine configurations that reduce external access to the information being processed, or arrangements that alert the operator to the presence of others.

c. Using certain specific machines to process personal data.

d. Any other physical safeguards, to include special technical arrangements that will protect the data during processing.

3. Other safeguards may include:

a. Using only certain selected operators to process personal data.

b. Processing personal data only at certain times during the day without the WPC manager's specific authorization.

c. Using only certain tapes or diskettes to process and store personal data.

d. Using continuous tapes for dictation of personal data.

e. Requiring all WPC copies of documents to be marked specifically so as to prevent inadvertent compromise.

f. Returning extra copies and mistakes to the customer with the product.

g. Disposing of waste containing personal data in a special manner.

h. Any other local procedures that provide adequate protection to the data being processed.

E. SAFEGUARDING INFORMATION DURING RETURN. The WPC shall protect the data until it is returned to the customer or is placed into a formal distribution channel. In conjunction with the appropriate administrative support personnel and the WPC customers, the WPC manager will establish procedures that protect the information from the time word processing is completed until it is returned to the customer. Safeguarding procedures may include:

1. Releasing products only to specifically identified individuals.

2. Using sealed envelopes to transmit products to the customer.

3. Using special cover sheets to protect products similar to the one discussed above.

4. Handcarrying products to the customers.

5. Using special messengers to return the products.

6. Any other procedures that adequately protect products from compromise while they are awaiting return or being returned to the customer.

F. SAFEGUARDS DURING STORAGE. The WPC manager shall ensure that all personal data retained in the center for any purpose (including samples) are protected properly. Safeguarding procedures may include:

1. Marking all hard copies retained with special legends or designators.

2. Storing media containing personal data in separate files or areas.

3. Marking the storage containers for media containing personal data with special legends or notations.

4. Restricting the reuse of media used to process personal data or erasing the media before reuse.

5. Establishing special criteria for the WPC retention of media used to store and process personal data.

6. Returning the media to the customer for retention with the file copies of the finished products.

7. Discouraging, when practical, the long-term storage of personal data in any form within the WPC.

8. Any other filing or storage procedures that safeguard adequately any personal information retained or filed within the WPC.

G. RISK ASSESSMENT FOR WPCs

1. Each WPC manager will ensure that a formal, written risk assessment is prepared for each WPC that processes personal information subject to this DLAR. The assessment will address the areas discussed in this enclosure, as well as any special risks that the WPC location, configuration, or organization may present to the compromise or alteration of personal data being processed or stored.

2. A risk assessment will be conducted at least every 5 years or whenever there is a change of equipment, equipment configuration, WPC location, WPC configuration or modification of the WPC facilities that either increases or decreases the likelihood or compromise of personal data.

3. Copies of the risk assessment will be retained by the WPC manager and made available to appropriate inspectors, as well as to personnel studying equipment for facility upgrading of personal data.

H. SPECIAL CONSIDERATIONS IN WPC DESIGN AND MODIFICATION. Procedures will be established to ensure that all personnel involved in the design of WPCs or the acquisition of word processing equipment are aware of the special considerations required when processing personal data subject to this DLAR.

OMB GUIDELINES FOR MATCHING PROGRAMS

A. PURPOSE. These guidelines supplement and will be used in conjunction with OMB Guidelines on the Administration of the Privacy Act of 1974, issued on July 1, 1975, and supplemented on November 21, 1975. They replace earlier guidance on conducting computerized matching programs issued on March 30, 1979. They are intended to help agencies relate the procedural requirements of the Privacy Act to the operational requirements of computerized matching. They are designed to address the concern expressed by the Congress in the Privacy Act of 1974 that "the increasing use of computers and sophisticated information technology, while essential to the efficient operation of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information." These guidelines do not authorize activities that are not permitted by law, nor do they prohibit activities expressly required to be performed by law. Complying with these guidelines, however, does not relieve a Federal agency of the obligation to comply with the provisions of the Privacy Act, including any provisions not cited in these guidelines.

B. SCOPE. These guidelines apply to all agencies subject to the Privacy Act of 1974 (5 U.S.C. 552a) and to all matching programs:

1. Performed by a Federal agency, whether the personal records used in the match are Federal or nonfederal.

2. For which a Federal agency discloses any personal records for use in a matching program performed by any other Federal agency or any nonfederal organization.

C. EFFECTIVE DATE. These guidelines were effective on May 11, 1982.

D. DEFINITIONS. For the purpose of the Guidelines, all the terms defined in the Privacy Act of 1974 apply.

1. Personal Record. Any information pertaining to an individual that is stored in an automated system of records; for example, a data base which contains information about individuals that is retrieved by name or some other personal identifier.

2. Matching Program. A procedure in which a computer is used to compare two or more automated systems of records or a system of records with a set of nonfederal records to find individuals who are common to more than one system or set. The procedure includes all of the steps associated with the match, including obtaining the records to be matched, actual use of the computer, administrative and investigative action on the hits, and disposition of the personal records maintained in connection with the match. It should be noted that a single matching program may involve several matches among a number of participants. Matching programs do not include the following:

4. Disposition of Records

a. Matching agencies will return or destroy source matching files (by mutual agreement) immediately after the match.

b. Records relating to this will be kept only so long as an investigation, either criminal or administrative, is active, and will be disposed of in accordance with the requirements of the Privacy Act and the Federal Records Act.

5. Publication Requirements

a. Agencies, before disclosing records outside the agency, will publish appropriate "routine use" notices in the Federal Register, if necessary.

b. If the matching program will result in the creation of a new or the substantial alteration of an existing system of records, the agency involved should publish the appropriate Federal Register notice and submit the requisite report to OMB and the Congress pursuant to OMB Circular No. A-108.

6. Reporting Requirements

a. As close to the initiation of the matching program as possible, matching agencies will publish in the Federal Register a brief public notice describing the matching program. The notice should include:

(1) The legal authority under which the match is being conducted.

(2) A description of the matching program including whether the program is one time or continuing, the organizations involved, the purpose or purposes for which the program is being conducted, and the procedures to be used in matching and following up on the "hits."

(3) A complete description of the personal records to be matched, including the source or sources, system of records identifying data, date or dates and page number of the most recent Federal Register full text publication when appropriate.

(4) The projected start and ending dates of the program.

(5) The security safeguards to be used to protect against unauthorized access or disclosure of the personal records.

(6) Plans for disposition of the source records and "hits."

7. Agencies should send a copy of this notice to the Congress and to OMB at the same time it is sent to the Federal Register.

a. Agencies should report new or altered systems of records as described in subparagraph 5b, above, as necessary.

b. Agencies should also be prepared to report on matching programs pursuant to the reporting requirements of either the Privacy Act or the Paperwork Reduction Act. Reports will be solicited by the Office of Information and Regulatory Affairs and will focus on both the protection of individual privacy and Government's effective use of information technology. Reporting instructions will be disseminated to the agencies as part of either the reports required by paragraph (p) of the Privacy Act, or Section 3514 of Public Law 96-511.

8. Use of Contractors. Matching programs should, as far as practicable, be conducted "in-house" by Federal agencies using agency personnel, rather than by contract. When contractors are used:

a. The matching agency should, consistent with paragraph (m) of the Privacy Act, cause the requirements of that Privacy Act to be applied to the contractor's performance of the matching program. The contract should include the Privacy Act clause required by Federal Personnel Regulation Amendment 155 (41 CFR 1-1.337-5).

b. The terms of the contract should include appropriate privacy and security provisions consistent with policies, regulations, standards, and guidelines issued by OMB, GSA, and the Department of Commerce.

c. The terms of the contract should preclude the contractor from using, disclosing, copying, or retaining records associated with the matching program for the contractor's own use.

d. Contractor personnel involved in the matching program shall be made explicitly aware of their obligations under the Privacy Act and of these guidelines, agency rules, and any special safeguards in relation to each specific match performed.

e. Any disclosures of records by the agency to the contractor should be made pursuant to a "routine use" (5 U.S.C. 552a (b)(3)).

F. IMPLEMENTATION AND OVERSIGHT. OMB will oversee the implementation of these guidelines and will interpret and advise upon agency proposals and actions within their scope, consistent with section 6 of the Privacy Act.

LITIGATION STATUS SHEET

1. Case Number[1/]
2. Requester
3. Document Title or Description[2/]
4. Litigation
   a. Date Complaint Filed
   b. Court
   c. Case File Number[1/]
5. Defendants (DoD Component and individual)
6. Remarks (brief explanation of what the case is about)
7. Court Action
   a. Court's Finding
   b. Disciplinary Action (as appropriate)
8. Appeal (as appropriate)
   a. Date Complaint File
   b. Court
   c. Case File Number[1/]
   d. Court's Finding
   e. Disciplinary Action (as appropriate)

[1/] Number used by the Component for reference purposes

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

PRIVACY ACT ENFORCEMENT ACTIONS

A. ADMINISTRATIVE REMEDIES. Any individual who feels he or she has a legitimate complaint or grievance against the Defense Logistics Agency or any DLA employee concerning any right granted by this DLAR will be permitted to seek relief through appropriate administrative channels.

B. CIVIL ACTIONS. An individual may file a civil suit against DLA or its employees if the individual feels certain provisions of the Privacy Act have been violated (see 5 U.S.C. 552a(g), reference (b)).

C. CIVIL REMEDIES. In addition to specific remedial actions, the Privacy Act provides for the payment of damages, court costs, and attorney fees in some cases.

D. CRIMINAL PENALTIES

1. The Privacy Act also provides for criminal penalties (see 5 U.S.C. 552a(1)). Any official or employee may be found guilty of a misdemeanor and fined not more than $5,000 if he or she willfully discloses personal information to anyone not entitled to receive the information, or maintains a system of records without publishing the required public notice in the Federal Register.

2. A person who requests or obtains access to any record concerning another individual under false pretenses may be found guilty of a misdemeanor and fined up to $5,000.

DLA EXEMPTION RULES

EXEMPTED RECORDS SYSTEMS. All systems of records maintained by the Defense Logistics Agency will 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 classifed under Executive Order 12356, 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 herein may contain isolated items of information which have been properly classified.

A. ID: S153.01 DLA-T (Specific Exemption)

1. Sys name: Personnel Security Files.

2. Exemption: This system of records is exempted from the following provisions of title 5, United States Code, section 552a: (c) (3); (d); and (e) (1).

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

4. Reasons: The investigatory reports are used by appropriate Security Officers and Commanders or other designated officials as a basis for determining a person's eligibility for access to information classified in the interests of national defense.

B. ID: S160.50 DLA(T) (Specific Exemption)

1. Sys name: Criminal Incident/Investigations File.

2. Exemption: This system of records is exempted from the following provisions of the Title 5, United States Code, section 552a: (c) (3); (d); and (e) (1).

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

4. Reasons: Granting individuals access to information collected and maintained by this component relating to the enforcement of criminal laws could interfere with orderly investigations, with the orderly administration of justice, and possibly enable suspects to avoid detection or apprehension. Disclosure of this information could result in the concealment, destruction or fabrication of evidence and jeopardize the safety and well being of informants, witnesses and their families, and law enforcement personnel and their families. Disclosure of this information could also reveal and render ineffectual investigative techniques, sources and methods used by this component and could result in the invasion of privacy of individuals only incidentally related to an investigation. Investigatory material is exempt to the extent that the disclosure of such material would reveal the identity of a source who furnished the information to the Government under an express promise that the identity of the source would be held in confidence, or prior to September 27, 1975 under an implied promise that the identity of the source would be held in confidence. This exemption will protect the identities of certain sources who would be otherwise unwilling to provide information to the Government. The exemption of the individual's right of access to his records and the reasons therefor necessitate the exemptions of this system of records from the requirements of the other cited provisions.

*U.S. GOVERNMENT PRINTING OFFICE: 1985-461-164:20007