

that the identity of the source would be held in confidence.

(vi) 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.

(vii) 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 September 27, 1975, 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.

(viii) Exemption rules for DLA systems of records are published in appendix H of this part.

(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 appendix E). 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 docu-

mentation 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 a 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.

§ 323.6 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.

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

A. *System identification.* See DLAH 5400.1.⁵

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 provided 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 location, list each location by category.

⁵Copies may be obtained, if needed, from the Defense Logistics Agency, ATTN: DLA-XP, Cameron Station, Alexandria, VA 22304.

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 5400.1.⁶ DLA-XA will obtain information concerning format requirements for preparation of an address directory from the 1st Information Systems Group (IISG), Room 3A-1066, The Pentagon, Washington, DC 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 the 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 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 (32 CFR part 359), 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 re-

sponsibility 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 use 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 5400.1⁷ apply to all systems notices unless the individual system notice specifically states that one or more 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 these responsible for safeguards (such as storage in safes, vaults, locked cabinets or rooms, use of guards, visitors 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

⁶Copies may be obtained, if needed, from the Defense Logistics Agency, ATTN: DLA-XP, Cameron Station, Alexandria, VA 22304.

⁷Copies may be obtained, if needed, from the Defense Logistics Agency, ATTN: DLA-XP, Cameron Station, Alexandria, VA 22304.

to DLAM 5015.1,⁸ 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) 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 part.

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 32 CFR part.") (DLAR 5400.21).

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 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 32 CFR part 323.") (DLAR 5400.21).

[DLAR 5400.21, 51 FR 33595, Sept. 22, 1986. Redesignated and amended at 56 FR 57803, Nov. 14, 1991]

APPENDIX B TO PART 323—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

⁸Copies may be obtained, if needed, from the Defense Logistics Agency, ATTN: DLA-XP, Cameron Station, Alexandria, VA 22304.

single PLFA's enlisted personnel to include all of DLA enlisted personnel would be considered an alteration).

d. A reduction in the number of individual 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).

b. Any change under this criteria requires a change in the "Retrievability" caption of the system notice.

c. If the records are no longer retrieved by name or personal identifier, cancel the system notice.

4. A change in the purpose for which the information in the system is used.

a. The new purpose must not be compatible with the existing purposes for which the system is maintained or a use that would not reasonably be expected to be an alteration.

b. If the use is compatible and reasonably expected, there is no change in purpose and no alteration occurs.

c. Any change under this criterion requires a change in the "Purpose(s)" caption and may require a change in the "Authority for maintenance of the system" caption.

5. Changes that alter the computer environment (such as changes to equipment configuration, software, or procedures) so as to create the potential for greater or easier access.

a. Increasing the number of offices with direct access is an alteration.

b. Software releases, such as operating systems and system utilities that provide for easier access are considered alterations.

c. The addition of an on-line capability to a previously batch-oriented system is an alteration.

d. The addition of peripheral devices such as tape devices, disk devices, card readers, printers, and similar devices to an existing

ADP system constitute an amendment if system security is preserved.

e. Changes to existing equipment configuration with on-line capability need not be considered alterations to the system if:

(1) The change does not alter the present security posture.

(2) The addition of terminals does not extend the capacity of the current operating system and existing security is preserved.

f. The connecting of two or more formerly independent automated systems or networks together creating a potential for greater access is an alteration.

g. Any change under this caption requires a change to the "Storage" caption element of the systems notice.

C. *Reports of new and altered systems.* Submit a report of a new or altered system to DLA-XA before collecting information and for using a new system or altering an existing system.

D. *Time restrictions on the operation of a new or altered system.* 1. All time periods begin from the date OSD signs the transmittal letters on the reports to OMB and Congress. The specific time limits are:

a. Sixty days must elapse before collection forms or formal instructions pertaining to the system may be issued.

b. Sixty days must elapse before the system may become operational.

c. Sixty days must elapse before any public issuance of a Request for Proposal or Invitation to Bid for a new ADP or telecommunication system.

NOTE: Requests for delegation of procurement authority may be submitted to the General Services Administration during the 60 days' waiting period, but these will include language that the Privacy Act reporting criteria have been reviewed and that a system report is required for such procurement.

d. Normally 30 days must elapse before publication in the FEDERAL REGISTER of the notice of a new or altered system and the preamble to the FEDERAL REGISTER notice must reflect the date the transmittal letters to OMB and Congress were signed by OSD.

2. Do not operate a system of records until the waiting periods have expired.

E. *Outside review of new and altered systems reports.* If no objections are received within 30 days of a submission to the President of the Senate, Speaker of the House of Representatives, and the Director, OMB, of a new or altered system report, it is presumed that the new or altered systems have been approved as submitted.

F. *Waiver of time restrictions.* 1. The OMB may authorize a Federal agency to begin operation of a system of records before the expiration of time limits described above. When seeking such a waiver, include in the letter of transmittal to DLA-XA an explanation why a delay of 60 days in establishing

the system of records would not be in the public interest. The transmittal must include:

- a. How the public interest will be affected adversely if the established time limits are followed.
 - b. Why earlier notice was not provided.
2. Under no circumstances will the routine uses for a new or altered system be implemented before 30 days have elapsed after publication of the system notice containing the routine uses in the FEDERAL REGISTER. This period cannot be waived.

APPENDIX C TO PART 323—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 part.
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 323) 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.

[DLAR 5400.21, 51 FR 33595, Sept. 22, 1986. Redesignated and amended at 56 FR 57803, Nov. 14, 1991]

APPENDIX D TO PART 323—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 in above.

4. Hand-carrying 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 will 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 regulation. 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.

APPENDIX E TO PART 323—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. Watching programs do not include the following:

a. Matches which compare a substantial number of records, such as, comparison of the Department of Education's defaulted student loan data base with the Office of Personnel Management's Federal employee data base would be covered; comparison of six individual student loan defaultees with the OPM file would not be covered.

b. Checks on specific individuals to verify data in an application for benefits done reasonably soon after the application is received.

c. Checks on specific individuals based on information which raises questions about an individual's eligibility for benefits or payments done reasonably soon after the information is received.

d. Matches done to produce aggregate statistical data without any personal identifiers.

e. Matches done to support any research or statistical project when the specific data are not to be used to make decisions about the rights, benefits, or privileges of specific individuals.

f. Matches done by an agency using its own records.

3. *Matching Agency.* The Federal agency which actually performs the match.

4. *Source Agency.* The Federal agency which discloses records from a system of records to be used in the match. Note that in some circumstances a source agency may be the instigator and ultimate beneficiary of the matching program, as when an agency lacking computer resources uses another agency to perform the match. The disclosure of records to the matching agency and any later disclosure of "hits" (by either the matching or the source agencies) must be

done in accordance with the provisions of paragraph (b) of the Privacy Act.

5. *Hit.* The identification, through a matching program, of a specific individual.

E. *Guidelines for Agencies Participating in Matching Programs.* Agencies should acquire and disclose matching records and conduct matching programs in accordance with the provisions of this section and the Privacy Act.

1. *Disclosing Personal Records for Matching Programs—*

a. *To another Federal agency.* Source agencies are responsible for determining whether or not to disclose personal records from their systems and for making sure they meet the necessary Privacy Act disclosure provisions when they do. Among the factors source agencies should consider are:

- (1) Legal authority for the match.
- (2) Purpose and description of the match.
- (3) Description of the records to be matched.
- (4) Whether the record subjects have consented to the match; or whether disclosure of records for the match would be compatible with the purpose for which the records were originally collected; that is, whether disclosure under a “routine use” would be appropriate; whether the soliciting agency is seeking the records for a legitimate law enforcement activity—whichever is appropriate; or any other provision of the Privacy Act under which disclosure may be made.
- (5) Description of additional information which may be subsequently disclosed in relation to “hits.”
- (6) Subsequent actions expected of the source (for example, verification of the identity of the “hits” or followup with individuals who are “hits”).
- (7) Safeguards to be afforded the records involved, including disposition.

b. If the agency is satisfied that disclosure of the records would not violate its responsibilities under the Privacy Act, it may proceed to make the disclosure to the matching agency. It should ensure that only the minimum information necessary to conduct the match is provided. If disclosure is to be made pursuant to a “routine use” (Section b.3. of the Privacy Act), it should ensure that the system of records contains such a use, or it should publish a routine use notice in the FEDERAL REGISTER. The agency should also be sure to maintain an accounting of the disclosure pursuant to Section (c) of the Privacy Act.

c. *To a nonfederal entity.* Before disclosing records to a nonfederal entity for a matching program to be carried out by that entity, a source agency should, in addition to all of the consideration in subparagraph a, above, also make reasonable efforts, pursuant to Section (e)(6) of the Privacy Act, to “assure that such records are accurate, complete, timely, and relevant for agency purposes.”

2. *Written Agreements.* Before disclosing to either a Federal or non-Federal entity, the source agency should require the matching entity to agree in writing to certain conditions governing the use of the matching file; for example, that the matching file will remain the property of the source agency and be returned at the end of the matching program (or destroyed as appropriate); that the file will be used and accessed only to match the file or files previously agreed to; that it will not be used to extract information concerning “non-hit” individuals for any purpose, and that it will not be duplicated or disseminated within or outside the matching agency unless authorized in writing by the source agency.

3. *Performing Matching Programs—*

a. Matching agencies should maintain reasonable administrative, technical, and physical security safeguards on all files involved in the matching program.

b. Matching agencies should ensure that they have appropriate systems of records including those containing “hits,” and that such systems and any routine uses have been appropriately notices in the FEDERAL REGISTER and reported to OMB and the Congress.

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 Pub. L. 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.

APPENDIX F TO PART 323—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).

APPENDIX G TO PART 323—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 cost, and attorney fees in some cases.

D. Criminal Penalties—

1. The Privacy Act also provides for criminal penalties (see 5 U.S.C. 552a(l).) 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.

¹Number used by the Component for reference purposes.

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

APPENDIX H TO PART 323—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 classified under Executive Order 12958 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: S500.10 DLA-I (Specific exemption).

1. *System 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 persons's eligibility for access to information classified in the interests of national defense.

b. ID: S500.20 DLA-I (Specific exemption).

1. *System 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 therefore necessitate the exemptions of this system of records from the requirements of the other cited provisions.

c. ID: S100.50 DLA-GC (Specific exemption).

1. *System name:* Fraud and Irregularities.
2. *Exemption:* This system of records is exempt from the provisions of 5 U.S.C. 552a(c)(3), (d)(1) through (4), (e)(1), (e)(4)(G), (H), and (I), and (f).
3. *Authorities:* 5 U.S.C. 552a(k)(2) and (k)(5).
4. *Reasons:* From subsection (c)(3) because granting access to the accounting for each disclosure as required by the Privacy Act, including the date, nature, and purpose of each disclosure and the identity of the recipient, could alert the subject to the existence of the investigation or prosecutive interest by DLA or other agencies. This could seriously compromise case preparation by prematurely revealing its existence and nature; compromise or interfere with witnesses or make witnesses reluctant to cooperate; and lead to suppression, alteration, or destruction of evidence.

From subsections (d)(1) through (d)(4) and (f) because providing access to records of a civil investigation and the right to contest the contents of those records and force changes to be made to the information contained therein would seriously interfere with and thwart the orderly and unbiased conduct of the investigation and impede case preparation. Providing access rights normally afforded under the Privacy Act would provide the subject with valuable information that would allow interference with or compromise of witnesses or render witnesses reluctant to cooperate; lead to suppression, alteration, or destruction of evidence; and result in the secreting of or other disposition of assets that would make them difficult or impossible to reach in order to satisfy any Government claim growing out of the investigation or proceeding.

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

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

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. DLA will, nevertheless, continue to publish such a notice in broad generic terms as is its current practice.

d. ID: S100.10 GC (Specific exemption).

1. *System name:* Whistleblower Complaint and Investigation Files.

2. *Exemption:* Portions of this system of records may be exempt under the provisions of 5 U.S.C. 552a(c)(3), (d)(1) through (d)(4), (e)(1), (e)(4)(G), (e)(4)(H), and (e)(4)(I), and (f).

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

4. *Reasons:* From subsection (c)(3) because granting access to the accounting for each disclosure as required by the Privacy Act, including the date, nature, and purpose of each disclosure and the identity of the recipient, could alert the subject to the existence of the investigation or prosecutive interest by DLA or other agencies. This could seriously compromise case preparation by prematurely revealing its existence and nature; compromise or interfere with witnesses or make witnesses reluctant to cooperate; and lead to suppression, alteration, or destruction of evidence.

From subsections (d)(1) through (d)(4), and (f) because providing access to records of a civil investigation and the right to contest the contents of those records and force changes to be made to the information contained therein would seriously interfere with and thwart the orderly and unbiased conduct of the investigation and impede case preparation. Providing access rights normally afforded under the Privacy Act would provide the subject with valuable information that would allow interference with or compromise of witnesses or render witnesses reluctant to cooperate; lead to suppression, alteration, or destruction of evidence; and result in the secreting of or other disposition of assets that would make them difficult or impossible to reach in order to satisfy any Government claim growing out of the investigation or proceeding.

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

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

in the system and to make amendments to and corrections of the information in the system. However, DLA will continue to publish such a notice in broad generic terms as is its current practice.

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. DLA will, nevertheless, continue to publish such a notice in broad generic terms as is its current practice.

e. ID: S500.60 CA (Specific exemption).

1. *System name:* DLA Complaint Program Records.

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

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

3. *Authority:* 5 U.S.C. 552a(k)(2) and (k)(5), subsections (c)(3), (d)(1) through (d)(4), (e)(1), (e)(4)(G), (H), and (I), and (f).

4. *Reasons:* (i) From subsection (c)(3) because to grant access to an accounting of disclosures as required by the Privacy Act, including the date, nature, and purpose of each disclosure and the identity of the recipient, could alert the subject to the existence of the investigation or prosecutive interest by DLA or other agencies. This could seriously compromise case preparation by prematurely revealing its existence and nature; compromise or interfere with witnesses or make witnesses reluctant to cooperate; and lead to suppression, alteration, or destruction of evidence.

(ii) From subsections (d)(1) through (d)(4), and (f) because providing access to records of a civil or administrative investigation and the right to contest the contents of those records and force changes to be made to the information contained therein would seriously interfere with and thwart the orderly and unbiased conduct of the investigation

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

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

(iv) From subsections (e)(4)(G) and (H) because 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. DLA will, nevertheless, continue to publish such a notice in broad generic terms as is its current practice.

[DLAR 5400.21, 51 FR 33595, Sept. 22, 1986. Re-designated at 56 FR 57803, Nov. 14, 1991, as amended at 55 FR 32913, Aug. 13, 1990; 57 FR 40609, Sept. 4, 1992; 59 FR 9668, Mar. 1, 1994; 60 FR 3088, Jan. 13, 1995; 61 FR 2916, Jan. 30, 1996; 63 FR 25772, May 11, 1998]

PART 324—DFAS PRIVACY ACT PROGRAM

Subpart A—General Information

- Sec.
324.1 Issuance and purpose.
324.2 Applicability and scope.
324.3 Policy.
324.4 Responsibilities.

Subpart B—Systems of Records

- 324.5 General information.
324.6 Procedural rules.
324.7 Exemption rules.

Subpart C—Individual Access to Records

- 324.8 Right of access.
324.9 Notification of record's existence.

- 324.10 Individual requests for access.
324.11 Denials.
324.12 Granting individual access to records.
324.13 Access to medical and psychological records.
324.14 Relationship between the Privacy Act and the Freedom of Information Act.

APPENDIX A TO PART 324—DFAS REPORTING REQUIREMENTS

APPENDIX B TO PART 324—SYSTEM OF RECORDS NOTICE

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

SOURCE: 61 FR 25561, May 22, 1996, unless otherwise noted.

Subpart A—General information

§324.1 Issuance and purpose.

The Defense Finance and Accounting Service fully implements the policy and procedures of the Privacy Act and the DoD 5400.11-R¹, 'Department of Defense Privacy Program' (see 32 CFR part 310). This regulation supplements the DoD Privacy Program only to establish policy for the Defense Finance and Accounting Service (DFAS) and provide DFAS unique procedures.

§324.2 Applicability and scope.

This regulation applies to all DFAS, Headquarters, DFAS Centers, the Financial System Organization (FSO), and other organizational components. It applies to contractor personnel who have entered a contractual agreement with DFAS. Prospective contractors will be advised of their responsibilities under the Privacy Act Program.

§324.3 Policy.

DFAS personnel will comply with the Privacy Act of 1974, the DoD Privacy Program and the DFAS Privacy Act Program. Strict adherence is required to ensure uniformity in the implementation of the DFAS Privacy Act Program and to create conditions that will foster public trust. Personal information maintained by DFAS organizational elements will be safeguarded. Information will be made available to the individual to whom it pertains to the maximum extent practicable. Specific

¹Copies may be obtained at cost from the National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.