Pt. 323, App. C

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.

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
Office of the Secretary of Defense

Pt. 323, App. 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.
   e. Using only certain selected operators to process personal data.
   f. Processing personal data only at certain times during the day without the WPC manager’s specific authorization.
   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.

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. 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.

Safeguards During Storage. The WPC manager shall ensure that all personal data...
A procedure in which

 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, 1978. 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.