

and each matching program must be justified individually in accordance with the OMB guidelines.

§310.111 Requesting matching programs.

(a) Forward all requests for matching programs to include necessary routine use amendments (see §310.62(i) of subpart G) and analysis and proposed matching program reports (see subsection E.6. of appendix I) to the Defense Privacy Office, ODASD(A).

(b) The Defense Privacy Office shall review each request and supporting material and forward the report and system notice amendments to the FEDERAL REGISTER, OMB, and Congress, as appropriate.

(c) Changes to existing matching programs shall be processed in the same manner as a new matching program report.

§310.112 Time limits for submitting matching reports.

(a) 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 (see §310.60(f) of subpart G).

(b) Submit the documentation required by §310.111(a) of this subpart to the Defense Privacy Office at least 45 days before the proposed initiation date of the matching program.

(c) The Defense Privacy Office may grant waivers to the 45 days' deadline for good cause shown. Requests for waivers shall be in writing and fully justified.

[51 FR 2364, Jan. 16, 1986. Redesignated at 56 FR 55631, Oct. 29, 1991, as amended at 56 FR 57801, Nov. 14, 1991]

§310.113 Matching programs among DoD components.

(a) For the purpose of the OMB guidelines, the Department of Defense and all DoD Components are considered a single agency.

(b) Before initiating a matching program using only the records of two or more DoD Components, notify the Defense Privacy Office that the match is to occur. The Defense Privacy Office

may request further information from the Component proposing the match.

(c) There is no need to notify the Defense Privacy Office of computer matches using only the records of a single Component.

§310.114 Annual review of systems of records.

The system manager 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.

APPENDIX A TO PART 310—SPECIAL CONSIDERATIONS FOR SAFEGUARDING PERSONAL INFORMATION IN ADP SYSTEMS

(See paragraph (b) of §310.13, subpart B)

A. General

1. The Automated Data Processing (ADP) environment subjects personal information to special hazards as to unauthorized compromise alteration, dissemination, and use. Therefore, special considerations must be given to safeguarding personal information in ADP systems.

2. Personal information must also be protected while it is being processed or accessed in computer environments outside the data processing installation (such as, remote job entry stations, terminal stations, minicomputers, microprocessors, and similar activities).

3. ADP facilities authorized to process classified material have adequate procedures and security for the purposes of this Regulation. However, all unclassified information subject to this Regulation must be processed following the procedures used to process and access information designated "For Official Use Only" (see "DoD Freedom of Information Act Program" (32 CFR part 286)).

B. Risk Management and Safeguarding Standards

1. Establish administrative, technical, and physical safeguards that are adequate to protect the information against unauthorized disclosure, access, or misuse (see Transmittal Memorandum No. 1 to OMB Circular A-71—Security of Federal Automated Information Systems).

2. Technical and physical safeguards alone will not protect against unintentional compromise due to errors, omissions, or poor procedures. Proper administrative controls generally provide cheaper and surer safeguards.

3. Tailor safeguards to the type of system, the nature of the information involved, and the specific threat to be countered.

C. Minimum Administrative Safeguard

The minimum safeguarding standards as set forth in paragraph (b) of §310.13, subpart B apply to all personal data within any ADP system. In addition:

1. Consider the following when establishing ADP safeguards:
 - a. The sensitivity of the data being processed, stored and accessed;
 - b. The installation environment;
 - c. The risk of exposure;
 - d. The cost of the safeguard under consideration.
2. Label or designate output and storage media products (intermediate and final) containing personal information that do not contain classified material in such a manner as to alert those using or handling the information of the need for special protection. Designating products "For Official Use Only" in accordance with subpart E of 32 CFR part 286, "DoD Freedom of Information Act Program," satisfies this requirement.
3. Mark and protect all computer products containing classified data in accordance with the DoD Information Security Program Regulation (32 CFR part 159) and the ADP Security Manual (DoD 5200.28-M).
4. Mark and protect all computer products containing "For Official Use Only" material in accordance with subpart E of 32 CFR part 286.
5. Ensure that safeguards for protected information stored at secondary sites are appropriate.
6. If there is a computer failure, restore all protected information being processed at the time of the failure using proper recovery procedures to ensure data integrity.
7. Train all ADP personnel involved in processing information subject to this part in proper safeguarding procedures.

D. Physical Safeguards

1. For all unclassified facilities, areas, and devices that process information subject to this part, establish physical safeguards that protect the information against reasonably identifiable threats that could result in unauthorized access or alteration.
2. Develop access procedures for unclassified computer rooms, tape libraries, micrographic facilities, decollating shops, product distribution areas, or other direct support areas that process or contain personal information subject to this part that control adequately access to these areas.
3. Safeguard on-line devices directly coupled to ADP systems that contain or process information from systems of records to prevent unauthorized disclosure use or alteration.

4. Dispose of paper records following appropriate record destruction procedures.

E. Technical Safeguards

1. The use of encryption devices solely for the purpose of protecting unclassified personal information transmitted over communication circuits or during processing in computer systems is normally discouraged. However, when a comprehensive risk assessment indicates that encryption is cost-effective it may be used.
2. Remove personal data stored on magnetic storage media by methods that preclude reconstruction of the data.
3. Ensure that personal information is not inadvertently disclosed as residue when transferring magnetic media between activities.
4. When it is necessary to provide dial-up remote access for the processing of personal information, control access by computer-verified passwords. Change passwords periodically or whenever compromise is known or suspected.
5. Normally the passwords shall give access only to those data elements (fields) required and not grant access to the entire data base.
6. Do not rely totally on proprietary software products to protect personnel data during processing or storage.

F. Special Procedures

1. System Managers shall:

- a. Notify the ADP manager whenever personal information subject to this Regulation is to be processed by an ADP facility.
- b. Prepare and submit for publication all system notices and amendments and alterations thereto (see paragraph (f) of §310.60 of subpart G).
- c. Identify to the ADP manager those activities and individuals authorized access to the information and notify the manager of any changes to the access authorizations.

2. ADP personnel shall:

- a. Permit only authorized individuals access to the information.
- b. Adhere to the established information protection procedures and rules of conduct.
- c. Notify the system manager and ADP manager whenever unauthorized personnel seek access to the information.

3. ADP installation managers shall:

- a. Maintain an inventory of all computer program applications used to process information subject to this part to include the identity of the systems of records involved.
- b. Verify that requests for new programs or changes to existing programs have been published as required (see paragraphs (a) and (b) of §310.63, subpart G).

c. Notify the system manager whenever changes to computer installations, communications networks, or any other changes in the ADP environment occur that require an altered system report be submitted (see paragraph (b) of §310.63, subpart G).

G. Record Disposal

1. Dispose of records subject to this part so as to prevent compromise (see paragraph (c) of §310.13 of subpart B). Magnetic tapes or other magnetic medium, may be cleared by degaussing, overwriting, or erasing. Unclassified carbon ribbons are considered destroyed when placed in a trash receptacle.

2. Do not use respliced waste computer products containing personal data.

H. Risk Assessment for ADP Installations That Process Personal Data

1. A separate risk assessment is not required for ADP installations that process classified material. A simple certification by the appropriate ADP official that the facility is cleared to process a given level of classified material (such as, Top Secret, Secret, or Confidential) and that the procedures followed in processing "For Official Use Only" material are to be followed in processing personal data subject to this Regulation is sufficient to meet the risk assessment requirement.

2. Prepare a formal risk assessment for each ADP installation (to include those activities with terminals and devices having access to ADP facilities) that processes personal information subject to this part and that do not process classified material.

3. Address the following in the risk assessment:

a. Identify the specific systems of records supported and determine their impact on the mission of the user.

b. Identify the threats (internal, external, and natural) to the data.

c. Determine the physical and operational (to include software) vulnerabilities.

d. Evaluate the relationships between vulnerabilities and threats.

e. Assess the impact of unauthorized disclosure or modification of the personal information.

f. Identify possible safeguards and their relationships to the threats to be countered.

g. Analyze the economic feasibility of adopting the identified safeguards.

h. Determine the safeguard to be used and develop implementation plans.

i. Discuss contingency plans including operational exercise plans.

j. Determine if procedures proposed are consistent with those identified in the system notices for system of records concerned.

k. Include a vulnerability assessment.

3. The risk assessment shall be reviewed by the appropriate Component officials.

4. Conduct a risk assessment at least every 5 years or when there is a change to the installation, its hardware, software, or administrative procedures that increase or decrease the likelihood of compromise or present new threats to the information.

5. Protect the risk assessment as it is a sensitive document.

6. Retain a copy of the risk assessment at the installation and make it available to appropriate inspectors and authorized personnel.

7. Include a summary of the current risk assessment with any report of new or altered system submitted in accordance with paragraph (c) of §310.63, subpart G, for any system from which information will be processed.

8. Complete a formal risk assessment at the beginning of the design phase for each new unclassified ADP installation and before beginning the processing of personal data on a regular basis in existing ADP facility that do not process classified data.

[51 FR 2364, Jan. 16, 1986. Redesignated at 56 FR 55631, Oct. 29, 1991, as amended at 56 FR 57801, Nov. 14, 1991]

APPENDIX B TO PART 310—SPECIAL CONSIDERATIONS FOR SAFEGUARDING PERSONAL INFORMATION DURING WORD PROCESSING

(See paragraph (b) of §310.13, subpart B)

A. Introduction

1. Normally, word processing support is provided under two general concepts. They are:

- a. Word processing centers (WPCs), and
- b. Work groups or clusters.

2. A WPC generally provides support to one or more functional areas. Characteristically, the customer delivers (by written draft or dictation) the information to be processed to the WPC. The WPC process the information and returns it to the customer. There are generally two types of WPCs.

a. A WPC may operate independent of the customer's function, providing service in much the same manner as a data processing installation provides ADP support, or a message center provides electronic message service, or

b. A WPC may work within a customer's function providing support to that function. The support being centralized in a WPC to take advantage of increased productivity.

3. A work group or cluster generally consists of one or more pieces of word processing equipment that are integrated into the functional office support system. The overall word processing and functional management may be one and the same. Depending on the size of the support job, there may be a work

group or cluster manager. Normally, however, they will be located within or in close proximity to the functional area supported. Information flows in and out of the work group or cluster by normal office routine and the personnel are an integral part of the office staff.

B. Minimum Standards of Protection

1. Regardless of configuration (WPC or work group), all personal data processed using word processing equipment shall be afforded the standards of protection required by paragraph (b) of §310.13, subpart B.

2. The remaining special considerations discussed in this appendix are primarily for WPCs operating independent of the customer's function. However, managers of other WPCs, work groups, and work clusters are encouraged to consider and adopt, when appropriate, the special considerations discussed herein.

3. WPCs that are not independent of a customer's function, work groups, and work clusters are not required to prepare formal written risk assessments (see section H., below).

C. WPC Information Flow

1. 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:

- a. Information receipt.
- b. Information processing.
- c. Information return.
- d. Information storage or filing.

2. WPCs do not control information acquisition or its ultimate use by the customers and, therefore, these are not addressed.

D. Safeguarding Information During Receipt

1. The word processing manager shall establish procedures.

a. That require each customer who requests that information subject to this part 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 part (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; or

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

b. To ensure that the operators or other WPC personnel receiving data for processing that has not been identified to be under the provisions of this part 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 that the customer has not identified as being in a system of records and that appears to meet the criteria set forth in paragraph (a) of §310.10, subpart B is called to the attention of the appropriate supervisory personnel and system manager.

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

E. Safeguarding Information During Processing

1. Each WPC supervisor shall establish internal safeguards that shall 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.

F. Safeguarding Information During Return

1. The WPC shall protect the data until it is returned to the customer or placed into a formal distribution channel.
2. In conjunction with the appropriate administrative support personnel and the WPC customers, the WPC manager shall establish procedures that protect the information from the time word processing is completed until it is returned to the customer.
3. Safeguarding procedures may include:
 - a. Releasing products only to specifically identifiable individuals;
 - b. Using sealed envelopes to transmit products to the customer;
 - c. Using special cover sheets to protect products similar to the one discussed in subparagraph D.1.a.(4), above;
 - d. Handcarrying products to the customers;
 - e. Using special messengers to return the products;
 - f. Any other procedures that protect adequately products from compromise while they are awaiting return or being returned to the customer.

G. Safeguards During Storage

1. The WPC manager shall ensure that all personal data retained in the center for any purpose (including samples) are protected properly.
2. Safeguarding procedures may include:
 - a. Marking all hard copies retained with special legends or designators;
 - b. Storing media containing personal data in separate files or areas;
 - c. Marking the storage containers for media containing personal data with special legends or notations;
 - d. Restricting the reuse of media used to process personal data or erasing automatically the media before reuse;
 - e. Establishing special criteria for the WPC retention of media used to store and process personal data;
 - f. Returning the media to the customer for retention with the file copies of the finished products;
 - g. Discouraging, when practical, the long-term storage of personal data in any form within the WPC;
 - h. Any other filing or storage procedures that safeguard adequately any personal information retained or filed within the WPC.

H. Risk Assessment for WPCs

1. Each WPC manager shall ensure that a formal, written risk assessment is prepared for each WPC that processes personal information subject to this part.
2. The assessment shall address the areas discussed in sections D., E., F., and G. of this appendix, as well as any special risks that the WPC location, configuration, or organization may present to the compromise or al-

teration of personal data being processed or stored.

3. A risk assessment shall 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 of compromise of personal data.
4. Copies of the assessment shall be retained by the WPC manager and made available to appropriate inspectors, as well as to personnel studying equipment for facility upgrading or modification.
5. Every new WPC shall have a formal risk assessment completed before beginning the processing of personal data.

I. Special Considerations in WPC Design and Modification

Procedures shall 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 part.

[51 FR 2364, Jan. 16, 1986. Redesignated at 56 FR 55631, Oct. 29, 1991, as amended at 56 FR 57801, Nov. 14, 1991]

APPENDIX C TO PART 310—DoD BLANKET ROUTINE USES

(See paragraph (e) of §310.41, subpart E)

A. Routine Use—Law Enforcement

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

B. Routine Use—Disclosure when Requesting Information

A record from a system of records maintained by a Component may be disclosed as a routine use to a federal, state, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a Component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

C. Routine Use—Disclosure of Requested Information

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

D. Routine Use—Congressional Inquiries

Disclosure from a system of records maintained by a Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

E. Routine Use—Private Relief Legislation

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

F. Routine Use—Disclosures Required by International Agreements

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

G. Routine Use—Disclosure to State and Local Taxing Authorities

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

H. Routine Use—Disclosure to the Office of Personnel Management

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

I. Routine Use—Disclosure to the Department of Justice for Litigation

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

J. Routine Use—Disclosure to Military Banking Facilities Overseas

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

K. Routine Use—Disclosure of Information to the General Services Administration (GSA)

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

L. Routine Use—Disclosure of Information to the National Archives and Records Administration (NARA)

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

Office of the Secretary of Defense

Pt. 310, App. D

M. Routine Use—Disclosure to the Merit Systems Protection Board

[See paragraph (d) of § 310.50, subpart F]

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

N. Routine Use-Counterintelligence Purpose

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

[51 FR 2364, Jan. 16, 1986. Redesignated at 56 FR 55631, Oct. 29, 1991, as amended at 56 FR 57801, Nov. 14, 1991; 62 FR 18518, Apr. 16, 1997]

APPENDIX D TO PART 310—PROVISIONS OF THE PRIVACY ACT FROM WHICH A GENERAL OR SPECIFIC EXEMPTION MAY BE CLAIMED

[See paragraph (d) of § 310.50, subpart F]

Exemption		Section of the Privacy Act
(j)(2)	(k)(1-7)	
No	No	(b)(1) Disclosures within the Department of Defense.
No	No	(2) Disclosures to the public.
No	No	(3) Disclosures for a "routine use."
No	No	(4) Disclosures to the Bureau of Census.
No	No	(5) Disclosures for statistical research and reporting.
No	No	(6) Disclosures to the National Archives.
No	No	(7) Disclosures for law enforcement purposes.
No	No	(8) Disclosures under emergency circumstances.
No	No	(9) Disclosures to the Congress.
No	No	(10) Disclosures to the General Accounting Office.
No	No	(11) Disclosures pursuant to court orders.
No	No	(12) Disclosure to consumer reporting agencies.
No	No	(c)(1) Making disclosure accountings.
No	No	(2) Retaining disclosure accountings.
Yes	Yes	(c)(3) Making disclosure accounting available to the individual.
Yes	No	(c)(4) Informing prior recipients of corrections.
Yes	Yes	(d)(1) Individual access to records.
Yes	Yes	(2) Amending records.

Exemption		Section of the Privacy Act
(j)(2)	(k)(1-7)	
Yes	Yes	(3) Review of the component's refusal to amend a record.
Yes	Yes	(4) Disclosure of disputed information.
Yes	Yes	(5) Access to information compiled in anticipation of civil action.
Yes	Yes	(e)(1) Restrictions on collecting information.
Yes	No	(e)(2) Collecting directly from the individual.
Yes	No	(3) Informing individuals from whom information is requested.
No	No	(e)(4)(A) Describing the name and location of the system.
No	No	(B) Describing categories of individuals.
No	No	(C) Describing categories of records.
No	No	(D) Describing routine uses.
No	No	(E) Describing records management policies and practices.
No	No	(F) Identifying responsible officials.
Yes	Yes	(e)(4)(G) Procedures for determining if a system contains a record on an individual.
Yes	Yes	(H) Procedures for gaining access.
Yes	Yes	(I) Describing categories of information sources.
Yes	No	(e)(5) Standards of accuracy.
No	No	(e)(6) Validating records before disclosure.
No	No	(e)(7) Records of first amendment activities.
No	No	(e)(8) Notification of disclosure under compulsory legal process.
No	No	(e)(9) Rules of conduct.
No	No	(e)(10) Administrative, technical and physical safeguards.
No	No	(11) Notice for new and revised routine uses.
Yes	Yes	(f)(1) Rules for determining if an individual is subject of a record.
Yes	Yes	(f)(2) Rules for handling access requests.
Yes	Yes	(f)(3) Rules for granting access.
Yes	Yes	(f)(4) Rules for amending records.
Yes	Yes	(f)(5) Rules regarding fees.
Yes	No	(g)(1) Basis for civil action.
Yes	No	(g)(2) Basis for judicial review and remedies for refusal to amend.
Yes	No	(g)(3) Basis for judicial review and remedies for denial of access.
Yes	No	(g)(4) Basis for judicial review and remedies for other failure to comply.
Yes	No	(g)(5) Jurisdiction and time limits.
Yes	No	(h) Rights of legal guardians.
No	No	(i)(1) Criminal penalties for unauthorized disclosure.
No	No	(2) Criminal penalties for failure to publish.
No	No	(3) Criminal penalties for obtaining records under false pretenses.
Yes ¹	No	(j) Rulemaking requirement.
N/A	No	(j)(1) General exemption for the Central Intelligence Agency.
N/A	No	(i)(2) General exemption for criminal law enforcement records.
Yes	N/A	(k)(1) Exemption for classified material.
N/A	N/A	(k)(2) Exemption for law enforcement material.
Yes	N/A	(k)(3) Exemption for records pertaining to Presidential protection.

Pt. 310, App. E

32 CFR Ch. I (7-1-98 Edition)

[See paragraph (d) of § 310.50, subpart F]

Exemption		Section of the Privacy Act
(j)(2)	(k)(1-7)	
Yes	N/A	(k)(4) Exemption for statistical records.
Yes	N/A	(k)(5) Exemption for investigatory material compiled for determining suitability for employment or service.
Yes	N/A	(k)(6) Exemption for testing or examination material.
Yes	N/A	(k)(7) Exemption for promotion evaluation materials used by the Armed Forces.
Yes	No	(l)(1) Records stored in NARA records centers.
Yes	No	(l)(2) Records archived before Sept. 27, 1975.
Yes	No	(l)(3) Records archived on or after Sept. 27, 1975.
Yes	No	(m) Applicability to Government contractors.
Yes	No	(n) Mailing lists.
Yes ¹	No	(o) Reports on new systems.
Yes ¹	No	(p) Annual report.

¹ See paragraph (d) of § 310.50, subpart F.

[51 FR 2364, Jan. 16, 1986. Redesignated at 56 FR 55631, Oct. 29, 1991, as amended at 56 FR 57801, Nov. 14, 1991; 62 FR 26389, May 14, 1997]

APPENDIX E TO PART 310—SAMPLE OF NEW OR ALTERED SYSTEM OF RECORDS NOTICE IN “FEDERAL REGISTER” FORMAT

(See paragraph (f) of § 310.60, subpart G)
 DEPARTMENT OF DEFENSE
 DEFENSE NUCLEAR AGENCY
 PRIVACY ACT OF 1974; NEW SYSTEM OF RECORDS
 AGENCY: Defense Nuclear Agency (DNA).
 ACTION: Notice of a new record system.

SUMMARY: The Defense Nuclear Agency is adding a new system of records to its inventory of systems of records subject to the Privacy Act of 1974. The system notice for the new system is set forth below.

DATES: This system shall be effective (30 days after publication in the Federal Register) unless comments are received which result in a contrary determination.

ADDRESS: Send comments to the System Manager identified in the system notice.

FOR FURTHER INFORMATION CONTACT: Robert L. Brittigan, General Counsel, Defense Nuclear Agency, Washington, DC 20305, Telephone (202) 325-7681.

SUPPLEMENTARY INFORMATION: The Defense Nuclear Agency record system notice as prescribed by the Privacy Act of 1974 (5 U.S.C. 552a), as amended, have appeared in the FEDERAL REGISTER on September 28, 1981 (46 FR 51073) and February 16, 1982 (47 FR 6829).

The Defense Nuclear Agency has submitted a new system report on March 27, 1982, for this system of records under the provisions of 5 U.S.C. 552a(o) of the Privacy Act.

Patricia H. Means,
 OSD Federal Register Liaison Officer, Department of Defense.

Sample

HDNA 609-03

System name: Personnel Exposed to Radiation from Nuclear Tests.

System Location: Headquarters, Defense Nuclear Agency, Washington, DC 20305, Main computer location.

Categories of individuals covered by the system: All DoD and DoD-affiliated personnel, military and civilian, who participated in the U.S. Government atmospheric nuclear test programs in the Pacific and at the Nevada Test Site.

Categories of records in the system: Personal information consisting of name, rank, service number, last known or current address, dates of test participation, exposure and unit of assignment.

Authority for maintenance of the system: 10 U.S.C. Section 133, Powers of an Executive Department of a Military Department to Prescribe Departmental Regulations; 10 U.S.C. Section 133, Secretary of Defense: Appointment, Powers, Duties and Delegation by; DoD Directive 5105.31, “Defense Nuclear Agency (DNA).”

Purpose(s): To identify those individuals who may have been exposed to radiation from nuclear atmospheric test conducted by the U.S. Government in the Pacific or at the Nevada Test Site.

Information is provided to the medical services of all the Military Departments to identify military and retired personnel who were exposed to ionizing radiator during testing.

Routine uses of records maintained in the system including categories of users, and the purpose of such uses:

To the National Research Council and Center for Disease Control to determine the effects of ionizing radiation for the limited purpose of conducting epidemiological studies of the atmospheric nuclear weapons tests on DoD participants in those tests.

To the Department of Energy (DoE) to identify DoE contractor personnel exposed to ionizing radiation during nuclear testing for the limited purpose of conducting epidemiological studies of radiation effects of individuals so identified.

To the Department of Transportation (DoT) for the limited purpose of identifying DoT and DoT-affiliated personnel exposed to ionizing radiation during nuclear testing.

To the Veterans Administration to make determinations on service-connected disability for the purpose of resolving claims.

Policies and Practices for storing, retrieving, accessing, retaining, and disposing of records in the system.

Storage: Paper records in file folders; computer magnetic tape disks and printouts in secure computer facility.

Retrievability: Paper records filed in folders and computer magnetic tape and disk retrieved by name.

Safeguards: Paper records are filed in folders stored in locked security safes. Magnetic tapes stored in a vault in a secure computer area.

Retention and disposal: Paper records are retained until information is transferred to magnetic tapes; then destroyed. Magnetic tapes and disks are retained indefinitely.

System manager(s) and address: Director, Defense Nuclear Agency, Attn.: Privacy Act Officer, Washington, DC 20305, telephone (202) 325-7681.

Notification procedure: Information may be obtained from the System Manager.

Record access procedures: Requests should be addressed to the System Manager.

Contesting record procedures: The agency's rules for contesting contents and appealing initial determinations are contained in DNA Instruction 5400.11 (32 CFR part 318). Additional information may be obtained from the System Manager.

Record source categories: DNA records, searches of DoD records by other DoD Components, and from individuals voluntarily contacting DNA by telephone or mail.

Systems exempted from certain provision of the Act: None.

[51 FR 2364, Jan. 16, 1986. Redesignated at 56 FR 55631, Oct. 29, 1991, as amended at 56 FR 57801, Nov. 14, 1991]

APPENDIX F TO PART 310—FORMAT FOR NEW OR ALTERED SYSTEM REPORT

(See paragraph (c) of §310.63, subpart G)

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

A. Transmittal Letter. The transmittal letter to the Director, Defense Privacy Office, ODASD(A), shall include any request for waivers as set forth in paragraph (g) of §310.63, subpart G. The narrative statement shall be attached thereto.

B. Narrative Statement. The narrative statement is typed in double space on standard bond paper in the format shown at attachment 1. The statement includes:

1. *System identification and name.* This caption sets forth the identification and name of the system (see paragraphs (b) and (c) of §310.62, subpart G).

2. *Responsible official.* The name, title, address, and telephone number of the privacy 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 paragraph (g) of §310.62, subpart G.

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 individual's First Amendment rights and the basis for maintaining it as provided for in paragraph (e) of §310.10, subpart B.

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 shall 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 Army procedural or exemption rules (32 CFR part 505) 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 (see paragraph (d) of §310.64, subpart G) an advance copy of the notice reflecting the specific changes proposed.

2. An advance copy of any new rules or changes to the published Component rules to be issued for the new or altered system. If no change to existing rules is required, so state in the narrative.

3. An advance copy of any proposed exemption rule if the new or altered system is to be exempted in accordance with subpart F. If

there is no exemption, so state in the narrative.

4. 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.

ATTACHMENT 1—SAMPLE FORMAT FOR
NARRATIVE STATEMENT

DEPARTMENT OF DEFENSE

(COMPONENT NAME)

REPORT ON NEW (OR ALTERED) SYSTEM
UNDER THE PRIVACY ACT OF 1974

(Indicate none or not applicable, as appropriate.)

1. *System Identification and name:*
2. *Responsible official:*
3. *Purpose(s) of the System:* (for a new system only) or *Nature of the Change(s) Proposed:* (for altered system).
4. *Authority for the System:*
5. *Number of Individuals:*
6. *Information on First Amendment Activities:*
7. *Measures to Ensure Information Accuracy:*
8. *Other Measures to Ensure System Security:*
9. *Relations to State or Local Government Activities:*
10. *Supporting Documentation:* (Indicate here, as a positive statement, those enclosures *not* required as set forth in section C. of the format instructions.)

SIGNATURE BLOCK OF SUBMITTING
OFFICIAL

ATTACHMENT 2—SAMPLE REPORT

DEPARTMENT OF DEFENSE

Defense Nuclear Agency

REPORT ON NEW SYSTEM UNDER THE
PRIVACY ACT OF 1974

1. *System Identification and Name:* HDNA 609-03, entitled "Personnel Exposed To Radiation From Nuclear Tests."
2. *Responsible Official:* Robert L. Brittigan, General Counsel, Defense Nuclear Agency, Washington, DC 20305. Telephone: Area Code 202 325-7781.
3. *Purpose(s) of the System:* To consolidate into one system the names, addresses, and exposures of all DoD or DoD-associated personnel who may have been exposed to ionizing radiation during the atmospheric nuclear testing programs in the Pacific and at the Nevada Test Site.
4. *Authority for the System:* See "Authority for Maintenance of the System" caption of the attached proposed system notice.
5. *Number of Individuals:* Approximately 300,00 individuals will be affected by this new system, since the system includes all DoD

and DoD-affiliated participants in the atmospheric nuclear tests program.

6. *Information on First Amendment Activities:* None.

7. *Measures to Ensure Information Accuracy:* Records consist of personal data to be provided by the individual such as name, rank, service number, last known or current address, dates of test participation, exposure date, if available, and unit of assignment. When the information has been obtained from sources other than the individual, follow-up is attempted to ensure accuracy.

8. *Other Measures to Ensure System Security:*
a. Paper records before processing for computer storage are retained in locked filing cabinets located in limited access facilities at DNA Headquarters and the Armed Forces Radiobiology Research Institute.

b. Privacy data in the Headquarters, DNA, ADP facility is afforded the same protection as classified data in that the DNA computer system employs a File Security System (FSS) to protect classified and privacy data files from being accessed by unauthorized user.

9. *Relations to State and Local Government Activities:* None

10. *Supporting Documentation:* No changes to existing procedural or exemption rules are required for this proposed new system.

Robert L. Brittigan
General Counsel

ENCLOSURES—2

1. Advance copy of proposed system notice.
2. Copy of tasking memorandum from the Assistant Secretary of Defense (Manpower, Reserve Affairs, and Logistics) to the Director, Defense Nuclear Agency, "DoD Personnel Participation in Atmospheric Nuclear Weapons Testing," January 28, 1978.

NOTE: Enclosures are not included in the sample, above.

[51 FR 2364, Jan. 16, 1986. Redesignated at 56 FR 55631, Oct. 29, 1991, as amended at 56 FR 57801, Nov. 14, 1991]

APPENDIX G TO PART 310—SAMPLE DELETIONS AND AMENDMENTS TO SYSTEMS NOTICES IN "FEDERAL REGISTER" FORMAT

(See paragraph (d) of §310.64, subpart G)

DEPARTMENT OF DEFENSE

Department of Air Force

PRIVACY ACT OF 1974; DELETIONS AND AMENDMENTS TO SYSTEMS OF RECORDS NOTICES
AGENCY: Department of the Air Force, DoD.
ACTION: Notice of deletions and amendments to systems of records.

Office of the Secretary of Defense

Pt. 310, App. G

SUMMARY: The Air Force proposes to delete three and amend two notices for systems of records subject to the Privacy Act of 1974. The specific changes to the notices being amended are set forth below followed by the system notices, as amended, published in their entirety.

DATES: These systems notices shall be amended as proposed without further notice on (30 days after publication in the FEDERAL REGISTER unless comments are received that would result in a contrary determination.

ADDRESS: Send comments to the system manager identified in the particular system notice concerned.

FOR FURTHER INFORMATION CONTACT: Mr. Jon E. Updike, HQ USAF/DAQD, The Pentagon, Washington, DC 20330-5024, Telephone: (202) 694-3431 Autovon: 224-3431

SUPPLEMENTARY INFORMATION: The Air Force systems of records notices inventory subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended, have been published to date in the FEDERAL REGISTER as follows:

FR Doc. 80-28255 (46 FR 50785) September 28, 1980

FR Doc. 80-31218 (46 FR 56774) October 28, 1980

FR Doc. 80-32284 (46 FR 58195) November 8, 1980

FR Doc. 80-33780 (46 FR 59996) November 23, 1980

The proposed amendments are not within the purview of the provisions of 5 U.S.C. 552a(o) which requires the submission of an altered system report.

Patricia H. Means,
OSD Federal Register Liaison Officer, Department of Defense.

DELETIONS

F01001 OQPTFLA

System name: Human Reliability for Special Missions.

Reason: This system is covered by F03004 AFDPMDB Advanced Personnel Data System (APDS) (46 FR 50821) August 28, 1981.

F01003 OBXQPCA

System name: Cadet Promotion List.

Reason: This system has been incorporated into F03502 AFA A Cadet Management System (46 FR 50875) July 28, 1981.

F01102 OYUEBLA

System name: Locator or Personnel Data file.

Reason: This system is covered by F01102 DAYX A Base, Unit, and Organizational Military and Civilian Personnel Locator Files (46 FR 50800) October 28, 1981.

AMENDMENTS

F03501 DPMDQIA

System name: Military Personnel Records System.

Changes:

System Location: In line 8, change "Adjustment" to Adjutant".

External users, uses and purposes:

Add at end:

"American National Red Cross. Information to local Red Cross offices for emergency assistance to military members, dependents, relatives, or other persons if conditions are compelling."

"Drug Enforcement Administration" (added to those agencies listed under Department of Justice).

"Department of Labor: Bureau of Employees' Compensation—medical information for claims of civilian employees formerly in military service; Employment and Training Administration—verification of service-related information for unemployment compensation claims; Labor-Management Services Administration—for investigations of possible violations of labor laws and pre-employment investigations; National Research Council—for medical research purposes; U.S. Soldiers' and Airmen's Home—service information to determine eligibility."

F03504 OJMPLSC

System name: Assessments Screening Records.

Changes:

System location: In line 1, change "3700 Personnel Processing Group" to "3507 Airman Classification Squadron."

Retention and disposal: Delete entry and substitute: "Records on airmen accepted for sensitive or high risk assignments are retained in the office files for 18 months, then destroyed. Records of nonselectees are retained in office files for 1 year, then destroyed. Destruction is by tearing into pieces, shredding, pulping, macerating, or burning."

Systems manager: In line 1, change "3700 PPGP (CCO)," to "3507 Airman Classification Squadron."

Record source categories: Add at end, "peers, character references, and the individual member."

[51 FR 2364, Jan. 16, 1986. Redesignated at 56 FR 55631, Oct. 29, 1991, as amended at 56 FR 57801, Nov. 14, 1991]

APPENDIX H TO PART 310—LITIGATION
STATUS SHEET

(See §310.104, subpart K)

1. Case Number.¹
2. Requester.
3. Document Title or Description.²
4. Litigation:
 - a. Date Complaint Filed.
 - b. Court.
 - c. Case File Number¹
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 Filed.
 - b. Court.
 - c. Case File Number.⁵
 - d. Court's Finding.
 - e. Disciplinary Action (as appropriate).

[51 FR 2364, Jan. 16, 1986. Redesignated at 56 FR 55631, Oct. 29, 1991, as amended at 56 FR 57801, Nov. 14, 1991]

APPENDIX I TO PART 310—OFFICE OF
MANAGEMENT AND BUDGET (OMB)
MATCHING GUIDELINES

(See §310.110, subpart L)

A. *Purpose.* These guidelines supplement and shall 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 concerns 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 fed-

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).

eral 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 are effective on May 11, 1982.

D. *Definitions.* For the purposes 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:

a. Matches that do not 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 follow-up 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 disclosures 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 paragraph E.1.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 nonfederal 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 insure that they have appropriate systems of records including those containing "hits," and that such systems and any routine uses have been appropriately noticed in the FEDERAL REGISTER and reported to OMB and the Congress, as appropriate.

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 hits 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 Schedule.

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 shall 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; and

(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 paragraph E.5.b., 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 the 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, however,

a. The matching agency should, consistent with paragraph (m) of the Privacy Act, cause the requirements of that 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 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 shall interpret and advise upon agency proposals and actions within their scope, consistent with section 6 of the Privacy Act.

[51 FR 2364, Jan. 16, 1986. Redesignated at 56 FR 55631, Oct. 29, 1991, as amended at 56 FR 57801, Nov. 14, 1991]

PART 311—OSD PRIVACY PROGRAM

Sec.

311.1 Reissuance and purpose.

311.2 Applicability and scope.

311.3 Definitions.

311.4 Policy.

311.5 Responsibilities.

311.6 Procedures.

311.7 Procedures for exemptions.

311.8 Information requirements.

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

SOURCE: 51 FR 7070, Feb. 28, 1986, unless otherwise noted. Redesignated at 56 FR 55631, Oct. 29, 1991.

§311.1 Reissuance and purpose.

This part reissues Administrative Instruction No. 81 to update and implement basic policies and procedures outlined in Privacy Act of 1974, DoD 5400.11-R, OMB Circular No. A-108 (TM No. 4) and to provide guidance and procedures for use in establishing the Privacy Program in the Office of the Secretary of Defense (OSD) and those organizations assigned to OSD for administrative support.

§311.2 Applicability and scope.

(a) This part applies to the OSD, Joint Staff, Defense Advanced Research Projects Agency (DARPA), Uniformed Services University of the Health Sciences (USUHS) and other activities assigned to OSD for administrative support (hereafter referred to collectively as "OSD Components").

(b) This part covers record systems maintained by OSD Components and