

irregularities, and significant problems. Also document remedial actions taken to correct problems identified.

(b) Retain inspections reports and later follow-up reports in accordance with established records disposition standards. These reports shall be made available to the Privacy Program officials concerned upon request.

Subpart K—Privacy Act Enforcement Actions

§ 310.100 Administrative remedies.

Any individual who feels he or she has a legitimate complaint or grievance against the Department of Defense or any DoD employee concerning any right granted by this part shall be permitted to seek relief through appropriate administrative channels.

§ 310.101 Civil actions.

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

§ 310.102 Civil remedies.

In addition to specific remedial actions, subsection (g) of the Privacy Act (5 U.S.C. 552a) provides for the payment of damages, court cost, and attorney fees in some cases.

§ 310.103 Criminal penalties.

(a) The Act also provides for criminal penalties (see 5 U.S.C. 552a(i)). Any official or employee may be found guilty of a misdemeanor and fined not more than \$5,000 if he or she willfully:

(1) Discloses personal information to anyone not entitled to receive the information (see subpart E); or

(2) Maintains a system of records without publishing the required public notice in the FEDERAL REGISTER (see subpart G).

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

§ 310.104 Litigation status sheet.

Whenever a complaint citing the Privacy Act is filed in a U.S. District Court against the Department of Defense, a DoD Component, or any DoD employee, the responsible system manager shall notify promptly the Defense Privacy Office, ODASD(A). The litigation status sheet at appendix H provides a standard format for this notification. The initial litigation status sheet forwarded shall, as a minimum, provide the information required by items 1 through 6. A revised litigation status sheet shall be provided at each stage of the litigation. When a court renders a formal opinion or judgment, copies of the judgment and opinion shall be provided to the Defense Privacy Office with the litigation status sheet reporting that judgment or opinion.

Subpart L—Matching Program Procedures

§ 310.110 OMB matching guidelines.

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 I). 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.

§ 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.

§ 310.112

(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.

32 CFR Ch. I (7-1-99 Edition)

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:

- The sensitivity of the data being processed, stored and accessed;
- The installation environment;
- The risk of exposure;
- The cost of the safeguard under consideration.