

§ 310.44

Components or the Component Inspector General.

§ 310.44 Inspection reporting.

(a) Document the findings of the inspectors in official reports that are furnished the responsible Component officials. These reports, when appropriate, shall reflect overall assets of the Component Privacy Program inspected, or portion thereof, identify deficiencies, 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 Violations

§ 310.45 Administrative remedies.

Any individual who believes 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.

§ 310.46 Civil actions.

An individual may file a civil suit against a DoD Component if the individual believes his or her rights under the Act have been violated. (See 5 U.S.C. 552a(g).)

§ 310.47 Civil remedies.

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

§ 310.48 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 information from a system of records, knowing dissemination is prohibited to anyone not entitled to receive the information (see subpart E of this part); or

(2) Maintains a system of records without publishing the required public

32 CFR Ch. I (7–1–11 Edition)

notice in the FEDERAL REGISTER. (See subpart G of this part.)

(b) Any person who knowingly and willfully 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.

§ 310.49 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 the DPO. The litigation status sheet at appendix H to this part 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 of the status sheet. 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 DPO with the litigation status sheet reporting that judgment or opinion.

§ 310.50 Lost, stolen, or compromised information.

(a) When a loss, theft, or compromise of information occurs (see § 310.14), the breach shall be reported to:

(1) The United States Computer Emergency Readiness Team (US CERT) within one hour of discovering that a breach of personally identifiable information has occurred. Components shall establish procedures to ensure that US CERT reporting is accomplished in accordance with the guidance set forth at <http://www.us-cert.gov>.

(i) The underlying incident that led to the loss or suspected loss of PII (e.g., computer incident, theft, loss of material, etc.) shall continue to be reported in accordance with established procedures (e.g., to designated Computer Network Defense (CND) Service Providers (reference (z)), law enforcement authorities, the chain of command, etc.).

(ii) [Reserved]

(2) The Senior Component Official for Privacy within 24 hours of discovering that a breach of personally identifiable

information has occurred. The Senior Component Official for Privacy, or their designee, shall notify the Defense Privacy Office of the breach within 48 hours upon being notified that a loss, theft, or compromise has occurred. The notification shall include the following information:

(i) Identify the Component/organization involved.

(ii) Specify the date of the breach and the number of individuals impacted, to include whether they are DoD civilian, military, or contractor personnel; DoD civilian or military retirees; family members; other Federal personnel or members of the public, etc.

(iii) Briefly describe the facts and circumstances surrounding the loss, theft, or compromise.

(iv) Briefly describe actions taken in response to the breach, to include whether the incident was investigated and by whom; the preliminary results of the inquiry if then known; actions taken to mitigate any harm that could result from the breach; whether the affected individuals are being notified, and if this will not be accomplished within 10 working days, that action will be initiated to notify the Deputy Secretary (see §310.14); what remedial actions have been, or will be, taken to prevent a similar such incident in the future, e.g., refresher training conducted, new or revised guidance issued; and any other information considered pertinent as to actions to be taken to ensure that information is properly safeguarded.

(2) The Component shall determine whether administrative or disciplinary action is warranted and appropriate for those individuals determined to be responsible for the loss, theft, or compromise.

Subpart L—Computer Matching Program Procedures

§ 310.51 General.

(a) A computer matching program covers two kinds of matching programs (see OMB Matching Guidelines, 54 FR 25818 (June 19, 1989)). If covered, the matches are subject to the requirements of this subpart. The covered programs are:

(1) Matches using records from Federal personnel or payroll systems of records, or

(2) Matches involving Federal benefits program if:

(i) To determine eligibility for a Federal benefit,

(ii) To determine compliance with benefit program requirements, or

(iii) To effect recovery of improper payments or delinquent debts under a Federal benefit program.

(b) The requirements of this part do not apply if matches are:

(1) Performed solely to produce aggregated statistical data without any personal identifiers. Personally identifying data can be used for purposes of conducting the match. However, the results of the match shall be stripped of any data that would identify an individual. Under no circumstances shall match results be used to take action against specific individuals.

(2) Performed to support research or statistical projects. Personally identifying data can be used for purposes of conducting the match and the match results may contain identifying data about individuals. However, the match results shall not be used to make a decision that affects the rights, benefits, or privileges of specific individuals.

(3) Performed by an agency, or a component thereof, whose principal function is the enforcement of criminal laws, subsequent to the initiation of a specific criminal or civil law enforcement investigation of a named individual or individuals.

(i) The match must flow from an investigation already underway which focuses on a named person or persons. "Fishing expeditions" in which the subjects are generically identified, such as "program beneficiaries" are not covered.

(ii) The match must be for the purpose of gathering evidence against the named individual or individuals.

(4) Performed for tax information-related purposes.

(5) Performed for routine administrative purposes using records relating to Federal personnel.

(i) The records to be used in the match must predominantly relate to Federal personnel (i.e., the percentage of records in the system of records that