AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

(1) *Orientation*. Training that provides basic understanding of this part as it applies to the individual's job performance. This training shall be provided to personnel, as appropriate, and should be a prerequisite to all other levels of training.

(2) *Specialized training*. Training that provides information as to the application of specific provisions of this part to specialized areas of job performance. Personnel of particular concern include, but are not limited to medical, personnel, and intelligence specialists, finance officers, DoD personnel who may be expected to deal with the news media or the public, special investigators, paperwork managers, and other specialists (reports, forms, records, and related functions), computer systems development personnel, computer systems operations personnel, statisticians dealing with personal data and program evaluations, contractors that will either operate systems of records on behalf of the Component or will have access to such systems incident to performing the contract, and anyone responsible for implementing or carrying out functions under this part.

(3) *Management*. Training designed to identify for responsible managers (such as, senior system managers, denial authorities, and decision-makers) considerations that they shall take into account when making management decisions regarding operational programs and activities having privacy implications.

(c) Include Privacy Act training in other courses of training when appropriate. Stress individual responsibilities and advise individuals of their rights and responsibilities under this part to ensure that it is understood that, where personally identifiable information is involved, individuals should handle and treat the information as if it was their information.

§ 310.38 Training methodology and procedures.

(a) Each DoD Component is responsible for the development of training procedures and methodology.

(b) The DPO shall assist the Components in developing these training programs and may develop privacy training programs for use by all DoD Components.

(c) Components shall conduct training as frequently as believed necessary so that personnel who are responsible for or are in receipt of information protected by 5 U.S.C. 552a are sensitive to the requirements of this part, especially the access, use, and dissemination restrictions. Components shall give consideration to whether annual training and/or annual certification should be mandated for all or specified personnel whose duties and responsibilities require daily interaction with personally identifiable information.

(d) Components shall conduct training that reaches the widest possible audience. Web-based training and video conferencing have been effective means to provide such training.

§ 310.39 Funding for training.

Each DoD Component shall fund its own privacy training program.

Subpart I—Reports

§ 310.40 Requirement for reports.

The DPO shall establish requirements for DoD Privacy Reports and the DoD Components may be required to provide data.

§ 310.41 Suspense for submission of reports.

The suspenses for submission of all reports shall be established by the DPO.

§ 310.42 Reports control symbol.

Any report established by this subpart in support of the Privacy Program shall be assigned Report Control Symbol DD–COMP(A)1379.

Subpart J—Inspections

§ 310.43 Privacy Act inspections.

During internal inspections, Component inspectors shall be alert for compliance with this part and for managerial, administrative, and operational problems associated with the implementation of the Defense Privacy Program. Programs shall be reviewed as frequently as considered necessary by

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 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