AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

transmittal letters are signed and dated.

(2) The system notice must be published in the FEDERAL REGISTER before a Component begins to operate the system (i.e., collect and use the information). If the new system has routine uses or the altered system adds a new routine use, no records may be disclosed pursuant to the routine use until the public has had 30 days to comment on the proposed use.

(3) The time periods run concurrently.

(e) *Exemptions for new systems.* See § 310.30(e) for the procedures to follow in submitting exemption rules for a new system of records or for submitting an exemption rule for an existing system of records.

§ 310.34 Amendment and deletion of system notices.

(a) *Criteria for an amended system notice.* (1) Certain minor changes to published systems notices are considered amendments and not alterations. (see § 310.33(b)).

(2) Amendments do not require a report of an altered system (see § 310.33(c)), but must be published in the FEDERAL REGISTER.

(b) *System notices for amended systems.* Components shall include the following when submitting an amendment for a system notice for publication in the FEDERAL REGISTER:

(1) The system identifier and name. (see § 310.32 (b) and (c)).

(2) A description of the nature and specific changes proposed.

(3) The full text of the system notice need not be submitted if the master registry contains a current system notice for the system. (see § 310.32(q)).

(c) *Deletion of system notices.* (1) Whenever a system is discontinued, combined into another system, or determined no longer to be subject to this part, a deletion notice is required.

(2) The notice of deletion shall include:

(i) The system identification and name.

(ii) The reason for the deletion.

(3) When the system is eliminated through combination or merger, identify the successor system or systems in the deletion notice.

(d) *Submission of amendments and deletions for publication.* (1) Submit amendments and deletions to the DPO for transmittal to the FEDERAL REGISTER for publication.

(2) Multiple deletions and amendments may be combined into a single submission.

Subpart H—Training Requirements

§ 310.35 Statutory training requirements.

The Privacy Act (5 U.S.C. 552a) requires each Agency to establish rules of conduct for all persons involved in the design, development, operation, and maintenance of any system of record and to train these persons with respect to these rules.

§ 310.36 OMB training guidelines.

The OMB guidelines (OMB Privacy Guidelines, 40 FR 28948 (July 9, 1975) require all agencies additionally to:

(a) Instruct their personnel in their rules of conduct and other rules and procedures adopted in implementing the Act, to ensure that they are reminded of their specific responsibilities for safeguarding personally identifiable information, the rules for acquiring and using such information, and the penalties for non-compliance.

(b) Incorporate training on the special requirements of the Act into both formal and informal (on-the-job) training programs.

§ 310.37 DoD training programs.

(a) The training shall include information regarding information privacy laws, regulations, policies and procedures governing the Department's collection, maintenance, use, or dissemination of personal information. The objective is to establish a culture of sensitivity to, and knowledge about, privacy issues involving individuals throughout the Department.

(b) To meet these training requirements, Components may establish three general levels of training for those persons, to include contractor personnel, who are involved in any way with the design, development, operation, or maintenance of privacy protected systems of records. These are:

(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