AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

to train the appropriate personnel with respect to the privacy rules including the penalties for non-compliance (See 5 U.S.C. 552a(e)(9)).

(2) To meet the training requirements, three general levels of training must be established. They are—

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

(ii) *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, personnel specialists, finance officers, DOD personnel who may be expected to deal with the news media or the public, special investigators, paperwork managers, individuals working with medical and security records, records managers, computer systems development personnel, computer systems operations personnel, statisticians dealing with personal data and program evaluations, contractors and anyone responsible for implementing or carrying out functions under this part. Specialized training should be provided on a periodic basis; and

(iii) *Managerial training*. Training designed to identify for responsible managers (such as senior system managers, Denial Authorities, and functional managers described in this section) issues that they should consider when making management decisions affected by the Privacy Act Program.

(b) *Training tools*. Helpful resources include—

(1) Privacy Act training slides for Major Commands and Privacy Act Officers: Contact the DA FOIA/P Office, or slides can be accessed at the Web site *https://www.rmda.belvoir.army.mil/rmdaxml/rmda/FPHomePage.asp*.

(2) The ''DOJ Freedom of Information Act Guide and Privacy Act Overview'': The U.S. Department of Justice, Executive Office for United States Attorneys, Office of Legal Education, 600 E. Street, NW., Room 7600, Washington, DC 20530, or training programs can be accessed at the Web site *www.usdoj.gov/usao/eousa/ole.html*.

§ 505.9 Reporting requirements.

The Department of the Army will submit reports, consistent with the requirements of DOD 5400.11–R, OMB Circular A–130, and as otherwise directed by the Defense Privacy Office. Contact the DA FOIA/P Office for further guidance regarding reporting requirements.

§ 505.10 Use and establishment of exemptions.

(a) *Three types of exemptions*. (1) There are three types of exemptions applicable to an individual's right to access permitted by the Privacy Act. They are the Special, General, and Specific exemptions.

(2) Special exemption (d)(5)—Relieves systems of records from the access provision of the Privacy Act only. This exemption applies to information compiled in reasonable anticipation of a civil action or proceeding.

(3) General exemption (j)(2)—Relieves systems of records from most requirements of the Act. Only Army activities actually engaged in the enforcement of criminal laws as their primary function may claim this exemption.

(4) Specific exemptions (k)(1)–(k)(7)–Relieves systems of records from only a few provisions of the Act.

(5) To find out if an exemption is available for a particular record, refer to the applicable system of records notices. System of records notices will state which exemptions apply to a particular type of record. System of records notices that are applicable to the Army are contained in DA Pam 25–51 (available at the Army Publishing Directorate Web site *http://www.usapa.army.mil/*), the Defense Privacy Office's Web site *http://www.defenselink.mil/privacy/*), or in this section). Some of the system of records notices apply only to the Army and the DOD and some notices are applicable government-wide.

(6) Descriptions of current exemptions are listed in detail at appendix C of this part.

(b) *Exemption procedures*. (1) For the General and Specific exemptions to be applicable to the Army, the Secretary

of the Army must promulgate exemption rules to implement them. This requirement is not applicable to the one Special exemption which is self-executing. Once an exemption is made applicable to the Army through the exemption rules, it will be listed in the applicable system of records notices to give notice of which specific types of records the exemption applies to. When a system manager seeks to have an exemption applied to a certain Privacy Act system of records that is not currently provided for by an existing system of records notice, the following information will be furnished to the DA FOIA/P Office—

(i) Applicable system of records notice;

(ii) Exemption sought; and

(iii) Justification.

(2) After appropriate staffing and approval by the Secretary of the Army and the Defense Privacy Office, it will be published in the FEDERAL REGISTER as a proposed rule, followed by a final rule 60 days later. No exemption may be invoked until these steps have been completed.

§ 505.11 Federal Register publishing requirements.

(a) *The Federal Register*. There are three types of documents relating to the Privacy Act Program that must be published in the FEDERAL REGISTER. They are the DA Privacy Program policy and procedures (AR 340–21), the DA exemption rules, and Privacy Act system of records notices.

(b) *Rulemaking procedures*. (1) DA Privacy Program procedures and exemption rules are subject to the formal rulemaking process.

(2) Privacy Act system of records notices are not subject to formal rulemaking and are published in the FEDERAL REGISTER as Notices, not Rules.

(3) The Privacy Program procedures and exemption rules are incorporated into the Code of Federal Regulations (CFR). Privacy Act system of records notices are not published in the CFR.

§ 505.12 Privacy Act enforcement actions.

(a) *Judicial sanctions*. The Act has both civil remedies and criminal penalties for violations of its provisions.

(1) *Civil remedies*. The DA is subject to civil remedies for violations of the Privacy Act. In addition to specific remedial actions, 5 U.S.C. 552a(g) may provide for the payment of damages, court costs, and attorney's fees.

(2) *Criminal penalties*. A DA official or employee may be found guilty of a misdemeanor and fined not more than $5,000 for willfully—

(i) Disclosing individually identifiable personal information to one not entitled to the information;

(ii) Requesting or obtaining information from another's record under false pretenses; or

(iii) Maintaining a system of records without first meeting the public notice requirements of the Act.

(b) *Litigation Status Sheet*. (1) When a complaint citing the Privacy Act is filed in a U.S. District Court against the Department of the Army, an Army Component, a DA Official, or any Army employee, the responsible system manager will promptly notify the Army Litigation Division, 901 North Stuart Street, Arlington, VA 22203–1837.

(2) The Litigation Status Sheet at appendix E of this part provides a standard format for this notification. At a minimum, the initial notification will have items (a) through (f) provided.

(3) A revised Litigation Status Sheet must be provided at each stage of the litigation.

(4) When a court renders a formal opinion or judgment, copies must be provided to the Defense Privacy Office by the Army Litigation Division.

(c) *Administrative remedies—Privacy Act complaints*. (1) The installation level Privacy Act Officer is responsible for processing Privacy Act complaints or allegations of Privacy Act violations. Guidance should be sought from the local Staff Judge Advocate and coordination made with the system manager to assist in the resolution of Privacy Act complaints. The local Privacy Act officer is responsible for—

(i) Reviewing allegations of Privacy Act violations and the evidence provided by the complainants;

(ii) Making an initial assessment as to the validity of the complaint, and taking appropriate corrective action;