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;

(iii) Coordinating with the local Staff Judge Advocate to determine whether a more formal investigation such as a commander's inquiry or an AR 15–6 investigation is appropriate; and

(iv) Ensuring the decision at the local level from either the Privacy Act Officer or other individual who directed a more formal investigation is provided to the complainant in writing.

(2) The decision at the local level may be appealed to the next higher command level Privacy Act Officer.

(3) A legal review from the next higher command level Privacy Act Officer's servicing Staff Judge Advocate is required prior to action on the appeal.

§ 505.13 Computer Matching Agreement Program.

(a) *General provisions.* (1) Pursuant to the Privacy Act and this part, DA records may be subject to computer matching, *i.e.*, the computer comparison of automated systems of records.

(2) There are two specific kinds of Matching Programs covered by the Privacy Act—

(i) Matches using records from Federal personnel or payroll systems of records; and

(ii) Matches involving Federal benefit programs to accomplish one or more of the following purposes—

(A) To determine eligibility for a Federal benefit;

(B) To comply with benefit program requirements; and

(C) To effect recovery of improper payments or delinquent debts from current or former beneficiaries.

(3) The comparison of records must be computerized. Manual comparisons are not covered.

(4) Any activity that expects to participate in a Computer Matching Program must contact the DA FOIA/P Office immediately.

(5) In all cases, Computer Matching Agreements are processed by the Defense Privacy Office and approved by the Defense Data Integrity Board. Agreements will be conducted in accordance with the requirements of 5 U.S.C. 552a, and OMB Circular A–130.

(b) *Other matching.* Several types of computer matching are exempt from the restrictions of the Act such as matches used for statistics, pilot programs, law enforcement, tax administration, routine administration, background checks, and foreign counterintelligence. The DA FOIA/P Office should be consulted if there is a question as to whether the Act governs a specific type of computer matching.

§ 505.14 Recordkeeping requirements under the Privacy Act.

(a) *AR 25–400–2, The Army Records Information Management System (ARIMS).* To maintain privacy records are required by the Army Records Information Management System (ARIMS) to provide adequate and proper documentation of the conduct of Army business so that the rights and interests of individuals and the Federal Government are protected.

(b) A full description of the records prescribed by this part and their disposition/retention requirements are found on the ARIMS Web site at *https://www.arims.army.mil.*

APPENDIX A TO PART 505—REFERENCES

(a) The Privacy Act of 1974 (5 U.S.C. 552a, as amended).

(b) OMB Circular No. A–130, Management of Federal Information Resources.

(c) AR 25–55, The Department of the Army Freedom of Information Program.

(d) DA PAM 25–51, The Army Privacy Program—System of Records Notices and Exemption Rules.

(e) DOD Directive 5400.11, Department of Defense Privacy Program.

(f) DOD 5400.11–R, Department of Defense Privacy Program.

(g) AR 25–2, Information Assurance

(h) AR 25–400–2, The Army Records Information Management System (ARIMS).

(i) AR 27–10, Military Justice.

(j) AR 40–66, Medical Record Administration and Health Care Documentation.

(k) AR 60–20 and AFR 147–14, Army and Air Force Exchange Service Operating Policies.

(l) AR 190–45, Law Enforcement Reporting.

(m) AR 195–2, Criminal Investigation Activities.

(n) AR 380–5, Department of Army Information Security Program.

(o) DOD Directive 5400–7, DOD Freedom of Information Act (FOIA) Program.

(q) DOD 5400.7–R, DOD Freedom of Information Program.

(r) DOD 6025.18–R, DOD Health Information Privacy Regulation (HIPAA).

(s) U.S. Department of Justice, Freedom of Information Act Guide and Privacy Act Overview.