

## Department of the Air Force, DoD

## § 806b.2

### Subpart E—Amending the Record

- 806b.21 Amendment reasons.
- 806b.22 Responding to amendment requests.
- 806b.23 Approving or denying a record amendment.
- 806b.24 Seeking review of unfavorable Agency determinations.
- 806b.25 Contents of Privacy Act case files.

### Subpart F—Appeals

- 806b.26 Appeal procedures.

### Subpart G—Privacy Act Notifications

- 806b.27 When to include a Privacy Act warning statement in publications.
- 806b.28 Warning banners.
- 806b.29 Sending personal information over electronic mail.

### Subpart H—Privacy Impact Assessments

- 806b.30 Evaluating information systems for Privacy Act compliance.

### Subpart I—Preparing and Publishing System Notices for the Federal Register

- 806b.31 Publishing System notices.
- 806b.32 Submitting notices for publication in the FEDERAL REGISTER.
- 806b.33 Reviewing notices.

### Subpart J—Protecting and Disposing of Records

- 806b.34 Protecting records.
- 806b.35 Balancing protection.
- 806b.36 Disposing of records.

### Subpart K—Privacy Act Exemptions

- 806b.37 Exemption types.
- 806b.38 Authorizing exemptions.
- 806b.39 Requesting an exemption.
- 806b.40 Exemptions.

### Subpart L—Disclosing Records to Third Parties

- 806b.41 Disclosure considerations.
- 806b.42 Social rosters.
- 806b.43 Placing personal information on shared drives.
- 806b.44 Personal information that requires protection.
- 806b.45 Releasable information.
- 806b.46 Disclosing other information.
- 806b.47 Rules for releasing Privacy Act information without the consent of the subject.
- 806b.48 Disclosing the medical records of minors.
- 806b.49 Disclosure accountings.
- 806b.50 Computer matching.
- 806b.51 Privacy and the Web.

### Subpart M—Training

- 806b.52 Who needs training?
- 806b.53 Training tools.
- 806b.54 Information collections, records, and forms or Information Management Tools (IMT).

APPENDIX A TO PART 806b—DEFINITIONS

APPENDIX B TO PART 806b—PREPARING A SYSTEM NOTICE

APPENDIX C TO PART 806b—DoD “BLANKET ROUTINE USES”

APPENDIX D TO PART 806b—GENERAL AND SPECIFIC EXEMPTIONS

APPENDIX E TO PART 806b—PRIVACY IMPACT ASSESSMENT

AUTHORITY: Pub. L. 93-579, 88 Stat. 1896 (5 U.S.C. 552a).

SOURCE: 69 FR 954, Jan. 7, 2004, unless otherwise noted.

## Subpart A—Overview of the Privacy Act Program

### § 806b.1 Summary of revisions.

This part moves responsibility for the Air Force Privacy Program from Air Force Communications and Information Center to the Air Force Chief Information Officer; prescribes Air Force Visual Aid 33-276, Privacy Act Label as optional; adds the *E-Gov Act of 2002* requirement for a Privacy Impact Assessment for all information systems that are new or have major changes; changes appeal processing from Air Force Communications and Information Center to Air Force Legal Services Agency; adds Privacy Act warning language to use on information systems subject to the Privacy Act, includes guidance on sending personal information via e-mail; adds procedures on complaints; and provides guidance on recall rosters; social rosters; consent statements, systems of records operated by a contractor, and placing information on shared drives.

### § 806b.2 Basic guidelines.

This part implements the *Privacy Act of 1974*<sup>1</sup> and applies to records on living U.S. citizens and permanent resident aliens that are retrieved by name or

<sup>1</sup> <http://www.usdoj.gov/04foia/privstat.htm>.

### § 806b.3

personal identifier. This part also provides guidance on collecting and disseminating personal information in general.

(a) Records that are retrieved by name or personal identifier are subject to Privacy Act requirements and are referred to as Privacy Act systems of records. The Air Force must publish notices in the FEDERAL REGISTER, describing the collection of information for new, changed or deleted systems to inform the public and give them an opportunity to comment before implementing or changing the system. (see appendix B to this part).

(b) An official system of records is:

(1) Authorized by law or Executive Order.

(2) Needed to carry out an Air Force mission or function.

(3) Published in the FEDERAL REGISTER.

(c) The Air Force will not:

(1) Keep records on how a person exercises First Amendment rights. Exceptions are when: The Air Force has the permission of that individual or is authorized by Federal statute; or the information pertains to, and is within the scope of, an authorized law enforcement activity. First Amendment rights include, but are not limited to, freedom of religion, freedom of political beliefs, freedom of speech, freedom of the press, the right to assemble, and the right to petition.

(2) Penalize or harass an individual for exercising rights guaranteed under the Privacy Act. We must reasonably help individuals exercise their rights under the Privacy Act.

(d) Air Force members will:

(1) Keep paper and electronic records that are retrieved by name or personal identifier only in approved Privacy Act systems published in the FEDERAL REGISTER.

(2) Collect, maintain, and use information in such systems, for purposes described in the published notice, to support programs authorized by law or Executive Order.

(3) Safeguard the records in the system and keep them the minimum time required.

(4) Ensure records are timely, accurate, complete, and relevant.

### 32 CFR Ch. VII (7-1-12 Edition)

(5) Amend and correct records on request.

(6) Allow individuals to review and receive copies of their own records unless the Secretary of the Air Force approved an exemption for the system; or the Air Force created the records in anticipation of a civil action or proceeding (5 U.S.C. 552a(d)(5)).

(7) Provide a review of decisions that deny individuals access to or amendment of their records through appellate procedures.

#### § 806b.3 Violation penalties.

An individual may file a civil law suit against the Air Force for failing to comply with the Privacy Act. The courts may find an individual offender guilty of a misdemeanor and fine that individual offender not more than \$5,000 for:

(a) Willfully maintaining a system of records that doesn't meet the public notice requirements.

(b) Disclosing information from a system of records to someone not entitled to the information.

(c) Obtaining someone else's records under false pretenses.

#### § 806b.4 Privacy Act complaints.

(a) Process Privacy Act complaints or allegations of Privacy Act violations through the appropriate base or Major Command Privacy Act office, to the local systems manager. The base or Major Command Privacy Act officer directs the process and provides guidance to the system manager. The local systems manager will investigate complaints, or allegations of Privacy Act violations; will establish and review the facts when possible; interview individuals as needed; determine validity of the complaint; take appropriate corrective action; and ensure a response is sent to the complainant through the Privacy Act Officer. In cases where no system manager can be identified, the local Privacy Act officer will assume these duties. Issues that cannot be resolved at the local level will be elevated to the Major Command Privacy Office. When appropriate, local system managers will also: refer cases for more formal investigation, refer cases for

command disciplinary action, and consult the servicing Staff Judge Advocate. In combatant commands, process component unique system complaints through the respective component chain of command.

(b) For Privacy Act complaints filed in a U.S. District Court against the Air Force, an Air Force activity, or any Air Force employee, Air Force Legal Services Agency, General Litigation Division (JACL) will provide Air Force Chief Information Officer/P a litigation summary to include: The case number, requester name, the nature of the case (denial of access, refusal to amend, incorrect records, or specify the particular violation of the Privacy Act), date complaint filed, court, defendants, and any appropriate remarks, as well as updates during the litigation process. When the court renders a formal opinion or judgment, Air Force Legal Services Agency, General Litigation Division (JACL) sends Air Force Chief Information Officer/P a copy of the judgment and opinion.

#### § 806b.5 Personal notes.

The Privacy Act does not apply to personal notes on individuals used as memory aids. Personal notes may become Privacy Act records if they are retrieved by name or other personal identifier and at least one of the following three conditions apply: Keeping or destroying the records is not at the sole discretion of the author; the notes are required by oral or written directive, regulation, or command policy; or they are shown to other agency personnel.

#### § 806b.6 Systems of records operated by a contractor.

Contractors who are required to operate or maintain a Privacy Act system of records by contract must follow this part for collecting, safeguarding, maintaining, using, accessing, amending and disseminating personal information. The record system affected is considered to be maintained by the Air Force and is subject to this part. Systems managers for offices who have contractors operating or maintaining such record systems must ensure the contract contains the proper Privacy Act clauses, and identify the record

system number, as required by the Defense Acquisition Regulation and this part.

(a) Contracts for systems of records operated or maintained by a contractor will be reviewed annually by the appropriate Major Command Privacy Officer to ensure compliance with this part.

(b) Disclosure of personal records to a contractor for use in the performance of an Air Force contract is considered a disclosure within the agency under exception (b)(1) of the Privacy Act (*see* § 806b.47(a)).

#### § 806b.7 Responsibilities.

(a) The Air Force Chief Information Officer is the senior Air Force Privacy Official with overall responsibility for the Air Force Privacy Act Program.

(b) The Office of the General Counsel to the Secretary of the Air Force, Fiscal and Administrative Law Division (GCA) makes final decisions on appeals.

(c) The General Litigation Division, Air Force Legal Services Agency (JACL), receives Privacy Act appeals and provides recommendations to the appellate authority. Service unique appeals, from combatant commands, should go through the respective chain of command.

(d) The Plans and Policy Directorate, Office of the Chief Information Officer manages the program through the Air Force Privacy Act Officer who:

(1) Administers procedures outlined in this part.

(2) Reviews publications and forms for compliance with this part.

(3) Reviews and approves proposed new, altered, and amended systems of records; and submits system notices and required reports to the Defense Privacy Office.

(4) Serves as the Air Force member on the Defense Privacy Board and the Defense Data Integrity Board.

(5) Provides guidance and assistance to Major Commands, field operating agencies, direct reporting units and combatant commands for which AF is executive agent in their implementation and execution of the Air Force Privacy Program. Ensures availability of training and training tools for a variety of audiences.

**§ 806b.8**

**32 CFR Ch. VII (7–1–12 Edition)**

(6) Provides advice and support to those commands to ensure that information requirements developed to collect or maintain personal data conform to Privacy Act standards; and that appropriate procedures and safeguards are developed, implemented, and maintained to protect the information.

(e) Major Command commanders, and Deputy Chiefs of Staff and comparable officials at Secretary of the Air Force and Headquarters United States Air Force offices implement this part.

(f) 11th Communications Squadron will provide Privacy Act training and submit Privacy Act reports for Headquarters United States Air Force and Secretary of the Air Force offices.

(g) Major Command Commanders: Appoint a command Privacy Act officer, and send the name, office symbol, phone number, and e-mail address to Air Force Chief Information Officer/P.

(h) Major Command and Headquarters Air Force Functional Chief Information Officers:

(1) Review and provide final approval on Privacy Impact Assessments (*see* appendix E of this part).

(2) Send a copy of approved Privacy Impact Assessments to Air Force Chief Information Officer/P.

(i) Major Command Privacy Act Officers:

(1) Train base Privacy Act officers. May authorize appointment of unit Privacy Act monitors to assist with implementation of the program.

(2) Promote Privacy Act awareness throughout the organization.

(3) Review publications and forms for compliance with this part (do forms require a Privacy Act Statement; is Privacy Act Statement correct?).

(4) Submit reports as required.

(5) Review system notices to validate currency.

(6) Evaluate the health of the program at regular intervals using this part as guidance.

(7) Review and provide recommendations on completed Privacy Impact Assessments for information systems.

(8) Resolve complaints or allegations of Privacy Act violations.

(9) Review and process denial recommendations.

(10) Provide guidance as needed to functionals on implementing the Privacy Act.

(j) Base Privacy Act Officers:

(1) Provide guidance and training to base personnel.

(2) Submit reports as required.

(3) Review publications and forms for compliance with this part.

(4) Review system notices to validate currency.

(5) Direct investigations of complaints/violations.

(6) Evaluate the health of the program at regular intervals using this part as guidance.

(k) System Managers:

(1) Manage and safeguard the system.

(2) Train users on Privacy Act requirements.

(3) Protect records from unauthorized disclosure, alteration, or destruction.

(4) Prepare system notices and reports.

(5) Answer Privacy Act requests.

(6) Records of disclosures.

(7) Validate system notices annually.

(8) Investigate Privacy Act complaints.

(1) System owners and developers:

(1) Decide the need for, and content of systems.

(2) Evaluate Privacy Act requirements of information systems in early stages of development.

(3) Complete a Privacy Impact Assessment and submit to the Privacy Act Officer.

**Subpart B—Obtaining Law Enforcement Records and Confidentiality Promises**

**§ 806b.8 Obtaining law enforcement records.**

The Commander, Air Force Office of Special Investigation; the Commander, Air Force Security Forces Center; Major Command, Field Operating Agency, and base chiefs of security forces; Air Force Office of Special Investigations detachment commanders; and designees of those offices may ask another agency for records for law enforcement under 5 U.S.C. 552a(b)(7). The requesting office must indicate in writing the specific part of the record desired and identify the law enforcement activity asking for the record.