

**§ 806b.20 Contents of Privacy Act case files.**

Do not keep copies of disputed records in this file. Use the file solely for statistics and to process requests. Do not use the case files to make any kind of determination about an individual. Document reasons for untimely responses. These files include:

- (a) Requests from and replies to individuals on whether a system has records about them.
- (b) Requests for access or amendment.
- (c) Approvals, denials, appeals, and final review actions.
- (d) Coordination actions and related papers.

**Subpart F—Privacy Act Notifications****§ 806b.21 When to include a Privacy Act warning statement in publications.**

Include a Privacy Act Warning Statement in each Air Force publication that requires collecting or keeping personal information in a system of records. Also include the warning statement when publications direct collection of the SSN from the individual. The warning statement will cite legal authority and the system of records number and title. You can use the following warning statement: 'This part requires collecting and maintaining information protected by the Privacy Act of 1974 authorized by (U.S.C. citation and or Executive Order number). System of records notice (number and title) applies.'

**§ 806b.22 Publishing system notices.**

The Air Force must publish notices in the FEDERAL REGISTER of new, amended, and deleted systems to inform the public of what records the Air Force keeps and give them an opportunity to comment. The Privacy Act also requires submission of new or significantly altered systems to the Office of Management and Budget (OMB) and both houses of the Congress before publication in the FEDERAL REGISTER. This includes:

- (a) Starting a new system.
- (b) Instituting significant changes to an existing system.

(c) Sending out data collection forms or instructions.

(d) Issuing a request for proposal or invitation for bid to support a new system.

**§ 806b.23 Timing of notices.**

At least 120 days before the effective start date, system managers must send the system notice to SAF/AAIA on a 5 1/4 or 3 1/2-inch disk in Wordstar (ASCII text file) or Microsoft Word, with a paper copy highlighting any changes through the MAJCOM or FOA Privacy Act Officer. See Appendix B of this part for a sample system notice.

**Subpart G—Protecting and Disposing of Records****§ 806b.24 Protecting records.**

Protect information according to its sensitivity level. Consider the personal sensitivity of the information and the risk of loss or alteration. Most information in systems of records is FOR OFFICIAL USE ONLY (FOUO). Refer to AFI 37-131<sup>2</sup>, 'Air Force Freedom of Information Act Program,' for protection methods.

**§ 806b.25 Balancing protection.**

Balance additional protection against risk and cost. AF Form 3227, 'Privacy Act Cover Sheet', is available for use with Privacy Act material. For example, a password may be enough protection for an automated system with a log-on protocol. Classified computer systems or those with established audit and password systems are obviously less vulnerable than unprotected files or word processors in offices that are periodically empty. Follow AFI 33-202<sup>3</sup>, 'The Air Force Computer Security Program,' for procedures on safeguarding personal information in automated records.

**§ 806b.26 Disposing of records.**

You may use the following methods to dispose of records protected by the Privacy Act according to records retention schedules:

<sup>2</sup>See footnote 1 to section 806b.11, of this part.

<sup>3</sup>See footnote 1 to section 806b.11, of this part.

(a) Destroy by any method that prevents compromise, such as tearing, burning, or shredding, so long as the personal data is not recognizable and beyond reconstruction.

(b) Degauss or overwrite magnetic tapes or other magnetic medium.

(c) Dispose of paper products through the Defense Reutilization and Marketing Office (DRMO) or through activities who manage a base-wide recycling program. The recycling sales contract must contain a clause requiring the contractor to safeguard privacy material until its destruction and to pulp, macerate, shred, or otherwise completely destroy the records. Originators must safeguard Privacy Act material until it is transferred to the recycling contractor. A federal employee or, if authorized, a contractor employee must witness the destruction. This transfer does not require a disclosure accounting.

### Subpart H—Privacy Act Exemptions

#### § 806b.27 Requesting an exemption.

A system manager who believes that a system needs an exemption from some or all of the requirements of the Privacy Act should send a request to SAF/AAIA through the MAJCOM or FOA Privacy Act Officer. The request should detail the reasons for the exemption and the section of the Act that allows the exemption. SAF/AAIA gets approval for the request through SAF/AA and the Defense Privacy Office.

#### § 806b.28 Exemption types.

(a) A general exemption frees a system from most parts of the Privacy Act.

(b) A specific exemption frees a system from only a few parts of the Privacy Act.

#### § 806b.29 Authorizing exemptions.

Only SAF/AA can exempt systems of records from any part of the Privacy Act. Denial authorities can withhold records using these exemptions only if SAF/AA previously approved and published an exemption for the system in the FEDERAL REGISTER. Appendix C of

this part lists the systems of records that have approved exemptions.

#### § 806b.30 Approved exemptions.

Approved exemptions exist under 5 U.S.C. 552a for:

(a) Certain systems of records used by activities whose principal function is criminal law enforcement (subsection (j)(2)).

(b) Classified information in any system of records (subsection (k)(1)).

(c) Law enforcement records (other than those covered by subsection (j)(2)). The Air Force must allow an individual access to any record that is used to deny rights, privileges or benefits to which he or she would otherwise be entitled by federal law or for which he or she would otherwise be eligible as a result of the maintenance of the information (unless doing so would reveal a confidential source) (subsection (k)(2)).

(d) Statistical records required by law. Data is for statistical use only and may not be used to decide individuals' rights, benefits, or entitlements (subsection (k)(4)).

(e) Data to determine suitability, eligibility, or qualifications for federal service or contracts, or access to classified information if access would reveal a confidential source (subsection (k)(5)).

(f) Qualification tests for appointment or promotion in the federal service if access to this information would compromise the objectivity of the tests (subsection (k)(6)).

(g) Information which the Armed Forces uses to evaluate potential for promotion if access to this information would reveal a confidential source (subsection (k)(7)).

### Subpart I—Disclosing Records to Third Parties

#### § 806b.31 Disclosure considerations.

Before releasing personal information to third parties, consider the consequences, check accuracy, and make sure that no law or directive bans disclosure. You can release personal information to third parties when the subject agrees orally or in writing. Air Force members consent to releasing