

Department of the Air Force, DoD

§ 806b.36

is implemented or changed. The Privacy Act also requires submission of new or significantly changed systems to the Office of Management and Budget and both houses of 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.32 Submitting notices for publication in the Federal Register.

At least 120 days before implementing a new system, or a major change to an existing system, subject to this part, system managers must send a proposed notice, through the Major Command Privacy Office, to Air Force Chief Information Officer/P. Send notices electronically to af.foia@pentagon.af.mil using Microsoft Word, using the Track Changes tool in Word to indicate additions/changes to existing notices. Follow the format outlined in appendix B to this part. For new systems, system managers must include a statement that a risk assessment was accomplished and is available should the Office of Management and Budget request it.

§ 806b.33 Reviewing notices.

System managers will review and validate their Privacy Act system notices annually and submit changes to Air Force Chief Information Officer/P through the Major Command Privacy Office.

Subpart J—Protecting and Disposing of Records

§ 806b.34 Protecting records.

Maintaining information privacy is the responsibility of every federal employee, military member, and contractor who comes into contact with information in identifiable form. Protect information according to its sensitivity level. Consider the personal sensitivity of the information and the risk of disclosure, loss or alteration. Most information in systems of records is

FOUO. Refer to DoD 5400.7-R/Air Force Supp, DoD Freedom of Information Act Program, for protection methods.

§ 806b.35 Balancing protection.

Balance additional protection against sensitivity, risk and cost. In some situations, a password may be enough protection for an automated system with a log-on protocol. Others may require more sophisticated security protection based on the sensitivity of the information. Classified computer systems or those with established audit and password systems are obviously less vulnerable than unprotected files. Follow Air Force Instruction 33-202, *Computer Security*,⁵ for procedures on safeguarding personal information in automated records.

(a) AF Form 3227, Privacy Act Cover Sheet,⁶ is optional and available for use with Privacy Act material. Use it to cover and protect personal information that you are using in office environments that are widely unprotected and accessible to many individuals. After use, such information should be protected as outlined in DoD 5400.7-R/Air Force Supp.

(b) Privacy Act Labels. Use of Air Force Visual Aid 33-276, Privacy Act Label, is optional to assist in protecting Privacy Act information on compact disks, diskettes, and tapes.

§ 806b.36 Disposing of records.

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

(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 or through activities that manage a base-wide recycling program.

⁵ <http://www.e-publishing.af.mil/pubfiles/af/33/afi33-202/afi33-202.pdf>.

⁶ <http://www.e-publishing.af.mil/formfiles/af/af3227/af3227.xfd>.

§ 806b.37

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 K—Privacy Act Exemptions

§ 806b.37 Exemption types.

There are two types of exemptions permitted by 5 U.S.C. 552a:

(a) A *General exemption* authorizes the exemption of a system of records from most parts of the Privacy Act.

(b) A *Specific exemption* authorizes the exemption of a system of records from only a few parts.

§ 806b.38 Authorizing exemptions.

Denial authorities may withhold records using Privacy Act exemptions only when an exemption for the system of records has been published in the FEDERAL REGISTER as a final rule. Appendix D lists the systems of records that have published exemptions with rationale.

§ 806b.39 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 will send a request to Air Force Chief Information Officer/P through the Major Command or Field Operating Agency Privacy Act Officer. The request will detail the reasons for the exemption, the section of the Act that allows the exemption, and the specific subsections of the Privacy Act from which the system is to be exempted, with justification for each subsection.

§ 806b.40 Exemptions.

Exemptions permissible under 5 U.S.C. 552a (subject to §806b.38 of this part):

(a) *The (j)(2) exemption*. Applies to investigative records created and main-

32 CFR Ch. VII (7–1–11 Edition)

tained by law-enforcement activities whose principal function is criminal law enforcement.

(b) *The (k)(1) exemption*. Applies to information specifically authorized to be classified under the DoD Information Security Program Regulation, 32 CFR part 159.

(c) *The (k)(2) exemption*. Applies to investigatory information compiled for law-enforcement purposes by nonlaw enforcement activities and which is not within the scope of Sec. 806b.40(a) of this part. However, 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).

(d) *The (k)(3) exemption*. Applies to records maintained in connection with providing protective services to the President and other individuals under 18 U.S.C. 3506.

(e) *The (k)(4) exemption*. Applies to records maintained solely for statistical research or program evaluation purposes and which are not used to make decisions on the rights, benefits, or entitlement of an individual except for census records which may be disclosed under 13 U.S.C. 8.

(f) *The (k)(5) exemption*. Applies to investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information, but only to the extent such material would reveal the identity of a confidential source. This provision allows protection of confidential sources used in background investigations, employment inquiries, and similar inquiries that are for personnel screening to determine suitability, eligibility, or qualifications.

(g) *The (k)(6) exemption*. Applies to testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal or military service, if the disclosure would compromise the objectivity or fairness of the test or examination process.