AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO



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*.