Chapter 4[3], provides additional guidance regarding For Official Use Only information.

(c) Do not disclose personal information to anyone outside DoD unless specifically authorized by the Privacy Act (see § 806b.47).

(d) Do not send Privacy Act information to distribution lists or group e-mail addresses unless each member has an official need to know the personal information. When in doubt, send only to individual accounts.

(e) Before forwarding e-mails you have received that contain personal information, verify that your intended recipients are authorized to receive the information under the Privacy Act (see § 806b.47).

Subpart H—Privacy Impact Assessments

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

Information system owners and developers must address Privacy Act requirements in the development stage of the system and integrate privacy protections into the development life cycle of the information system. This is accomplished with a Privacy Impact Assessment.

(a) The Privacy Impact Assessment addresses what information is to be collected; why the information is being collected; the intended use of the information; with whom the information will be shared; what notice or opportunities for the individual to decline or consent to providing the information collected, and how that information is shared; secured; and whether a system of records is being created, or an existing system is being amended. The E-Government Act of 2002[4] requires Privacy Impact Assessments to be conducted before:

(1) Developing or procuring information technology systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public.

(2) Initiating a new electronic collection of information in identifiable form for 10 or more persons excluding agencies, instrumentalities, or employees of the Federal Government.

(b) In general, Privacy Impact Assessments are required to be performed and updated as necessary where a system change creates new privacy risks.

(c) No Privacy Impact Assessment is required where information relates to internal government operations, has been previously assessed under an evaluation similar to a Privacy Impact Assessment, or where privacy issues are unchanged.

(d) The depth and content of the Privacy Impact Assessment should be appropriate for the nature of the information to be collected and the size and complexity of the information technology system.

(e) The system owner will conduct a Privacy Impact Assessment as outlined in appendix E to this part and send it to their Major Command Privacy Act office for review and final approval by the Major Command or Headquarters Air Force Functional Chief Information Officer. The Major Command or Headquarters Air Force Functional Chief Information Officer will send a copy of approved Privacy Impact Assessments to Air Force Chief Information Officer/P, 1155 Air Force Pentagon, Washington DC 20330–1155; or e-mail *af.foia@pentagon.af.mil*.

(f) Whenever practicable, approved Privacy Impact Assessments will be posted to the Freedom of Information Act/Privacy Act Web site for public access at *http://www.foia.af.mil* (this requirement will be waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment).

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

§ 806b.31 Publishing system notices.

The Air Force must publish notices in the FEDERAL REGISTER of new, changed, and deleted systems to inform the public of what records the Air Force keeps and give them an opportunity to comment before the system

[3] *http://www.dtic.mil/whs/directives/corres/pdf/54007r__0998/p54007r.pdf*.

[4] *http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107__cong__public__laws&docid=f:publ347.107.pdf*.

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*.