

This e-mail contains FOR OFFICIAL USE ONLY (FOUO) information which must be protected under the Privacy Act and AFI 33-332.

(b) Do not indiscriminately apply this statement to e-mails. Use it only in situations when you are actually transmitting personal information. DoD Regulation 5400.7/AF Supp, Chapter 4, provides additional guidance regarding FOUO 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 PA 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 PA 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 (PIA).

(a) The PIA 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 consent will be provided individuals regarding 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 requires PIAs to be conducted before:

(1) Developing or procuring information technology (IT) that collects, maintains, or disseminates information in identifiable form from or about members of the public.

(2) Initiating a new collection of information, using IT, that collects, maintains, or disseminates information in identifiable form for 10 or more persons excluding agencies, instrumentalities, or employees of the Federal Government.

(b) The system owner will conduct a PIA as outlined in Appendix F and send

it to their MAJCOM Privacy Act office for review and final approval by the MAJCOM or HAF Functional CIO. The MAJCOM or HAF Functional CIO will send a copy of approved PIAs to AF-CIO/P, 1155 Air Force Pentagon, Washington DC 20330-1155; or e-mail af.foia@pentagon.af.mil.

(c) Whenever practicable, approved PIAs will be posted to the FOIA/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).

(d) OMB requires agencies to submit copies of the PIA for each system for which funding is requested. AF-CIO/P will furnish OMB applicable PIAs through the Defense Privacy Office.

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 is implemented or changed. The PA also requires submission of new or significantly changed systems to the OMB 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 MAJCOM Privacy Office, to AF-CIO/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 D to this part. For new systems, system managers must include a statement that a risk assessment was accomplished and is available should the OMB request it.

§ 806b.33 Reviewing Notices.

System managers will review and validate their PA system notices annually and submit changes to AF-

CIO/P through the MAJCOM 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/AF 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 AFI 33-202, Computer Security, for procedures on safeguarding personal information in automated records.

(a) AF Form 3227, Privacy Act Cover Sheet, 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/AF Supp.

(b) Privacy Act Labels. Use of AFVA 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. The