

**20 SEPTEMBER 2001**



**Communications and Information**

**★EMPLOYEE RESPONSIBILITIES UNDER  
THE FREEDOM OF INFORMATION ACT (FOIA)  
AND THE PRIVACY ACT (PA)**

---

**NOTICE:** This publication is available digitally on the HQ AETC Publishing WWW site at: <http://www.aetc.randolph.af.mil/im>. If you lack access, contact your base publishing manager.

---

OPR: HQ AETC/SCMC (Ms P. Sekula)  
Supersedes AETCPAM 37-101, 14 June 1997

Certified by: HQ AETC/SCM (Mr P. Barrick)  
Pages: 6  
Distribution: F

---

This pamphlet implements AFD 37-1, *Air Force Information Management* (will become AFD 33-3). It is a helpful tool for AETC employees to use in carrying out their responsibilities as required by the FOIA and PA. However, it is not a substitute for official training required by the FOIA and PA. DoD 5400.7-R/AF Sup, *DoD Freedom of Information Act Program*, and AFI 33-332, *Air Force Privacy Act Program*, take precedence over this pamphlet. This pamphlet does not apply to the Air National Guard or Air Force Reserve Command.

Attachment 1 contains a glossary of references and supporting information. Maintain and dispose of records created as a result of prescribed processes in accordance with AFMAN 37-139, *Records Disposition Schedule* (will become AFMAN 33-322, Volume 4).

### **SUMMARY OF REVISIONS**

**This document is substantially revised and must be completely reviewed.**

#### **1. Introduction:**

1.1. The FOIA and PA place dual responsibilities on AETC, as follows:

1.1.1. Under the FOIA, AETC employees are required to disclose information the public has a “right to know,” unless the information is exempt according to one of the nine FOIA exemptions. **NOTE:** Chapter 3 of DoD 5400.7-R/AF Sup contains information about these exemptions.

1.1.2. Under the PA, AETC employees must safeguard an individual’s personal information against unauthorized disclosures.

1.2. This pamphlet discusses your responsibilities for the disclosure and protection of this information, as well as your rights under the FOIA and PA. Under the FOIA, you are viewed as a member of the

general public; under the PA, you are a federal employee entitled to the protection of your personal information maintained by the government.

## **2. Freedom of Information Act (FOIA) (DoD 5400.7-R/AF Sup):**

### **2.1. Basic Principles:**

2.1.1. The FOIA is an access statute that opens the business of government to the general public. The FOIA may be used by anyone, regardless of citizenship, to request copies of existing government records without giving a reason for the request.

2.1.2. Generally, all government information is subject to the FOIA. This includes the following: (1) *all* paper and electronic materials in your office (not just records maintained in the organization's official filing system), (2) information maintained in PA systems of records, and (3) your e-mail, word processing files, agency working files, etc. The public may inspect or obtain copies of all public filings ("public" records) maintained by an agency through public reference facilities or public web pages. However, requests for access to "nonpublic" agency records must be submitted in writing under the provisions of the FOIA.

2.1.3. The FOIA requires all federal agency records to be released to the public upon written request. **EXCEPTIONS:** Those records that fall within the scope of one of the nine specific exemptions or two specific law enforcement record exclusions are reasons an agency may deny access to the requester. For more information on these exemptions and exclusions, refer to DoD 5400.7-R/AF Sup, Chapter 3.

### **2.2. Responsibilities:**

2.2.1. The FOIA requires the government to *respond* to written requests for information within 20 workdays after receipt of the request. Therefore, when you or someone in your office receives a written FOIA request for agency records from anyone outside the organization, you are responsible for immediately hand-carrying or forwarding the request to your local base FOIA manager for processing.

2.2.2. If your office is the OPR for the records requested under the FOIA, you are responsible for conducting a thorough search for all the records (regardless of the media) and providing a written response to the FOIA office as quickly as possible.

2.2.3. Once a request has been received, all responsive information must be reviewed for release; no information may be destroyed. If you believe some or all of the information should not be released to the public, cite one of the nine FOIA exemptions found in DoD 5400.7-R/AF Sup and provide your written rationale for each exemption used. Your FOIA manager will help you determine which, if any, of the nine FOIA exemptions apply. For example, information does not have to be released if the release would jeopardize national security ([b][1]), reveal trade secrets or confidential business information ([b][4]), reveal the deliberative process of the Air Force ([b][5]), or cause an unwarranted invasion of personal privacy ([b][6] and [b][7][c]).

2.2.4. Remember, accurate recordkeeping is a must! To protect yourself from being held responsible by the court for an improper withholding, be sure to give the FOIA manager a copy of all records that are responsive to a FOIA request.

**2.3. Information Available in a FOIA Reading Room.** The FOIA manager at each AETC installation will establish a reading room where the public may inspect releasable records. When a FOIA office or an OPR receives (or anticipates receiving) five or more requests for the **same** record in a quarter (for example, a request for a list of government purchase cardholders), the office will consider the request a frequently requested record--according to FOIA-processed records ([a][2][D])--and make it publicly available in both paper and electronic form. For official use only (FOUO) and FOIA-exempt information should never be placed in these reading rooms. For more information on FOIA reading rooms, refer to DoD 5400.7-R/AF Sup, Chapter 2.

### **3. Privacy Act (PA) (AFI 33-332):**

**3.1. Basic Principles.** The Privacy Act of 1974 establishes safeguards for the protection of records the government collects and maintains on US citizens and lawfully admitted permanent residents. This act is a confidentiality and records management statute that protects information about people from public scrutiny. Specifically, it mandates that the government will:

3.1.1. Tell people (at the time it is collecting information about them) why this information is being collected and how it will be used.

3.1.2. Publish a notice in the *Federal Register* of new or revised systems of records on individuals. (No secret government record systems about people are permitted.)

3.1.3. Publish a notice in the *Federal Register* before conducting computer-matching programs.

3.1.4. Permit no secret use of the information the government has collected about people.

3.1.5. Safeguard the records in the system and keep those records timely, accurate, complete, and relevant.

3.1.6. Allow individuals to access records that pertain to them and allow them the right to correct such records.

### **3.2. PA Records:**

3.2.1. The PA applies to information in Air Force systems of records on living US citizens and permanent resident aliens. Although the PA does not protect the records of deceased individuals, the privacy of the surviving family members must be taken into consideration.

3.2.2. The PA defines a system of records as any group of agency records, in paper or electronic form, that contains information about people from which information is retrieved by a personal identifier, such as a person's name, social security number, patient identification number, fingerprints, voice print, etc.

3.2.3. Go to <http://www.defenselink.mil/privacy/notices/usaf> for a complete list of approved Air Force PA systems of records.

**3.3. Contractor-Operated Systems of Records.** Contractors who operate or maintain a system of records or a portion of a system for a DoD component are, for purposes of the PA, DoD employees and subject to the requirements of the PA. Compliance with PA, as well its access and disclosure provisions,

must be written into the contract in accordance with Part 24 of the *Federal Acquisition Regulation (FAR)*. Failure to comply could render DoD, not the contractor, liable.

### **3.4. Rights and Responsibilities:**

**3.4.1. Overview.** As a federal employee, you are entitled to the full protection and rights established by the PA. In addition to being protected by this act, federal employees who work with government records containing personal information are responsible for carrying out the requirements of the PA.

**3.4.2. Your Rights.** As an individual, you have a right to (1) access your own records, (2) know to whom your records have been disclosed, (3) request amendment to your records when they are not timely, relevant, accurate, or complete, and (4) seek redress in the courts if denied access to or amendment of your own records. The PA protects your records from unauthorized access and disclosure.

### **3.4.3. Your Responsibilities:**

3.4.3.1. Administrative, technical, and physical safeguards are required for records. Each AETC employee who handles PA records must adhere to the rules of conduct to protect the information from the possibility of unwarranted disclosure or access by unauthorized persons. This also includes the safeguarding of personal information in automated records.

3.4.3.2. Label physical media (such as diskettes, tapes, or other media) that contains PA material with Air Force Visual Aid (AFVA) 33-276, *Air Force Privacy Act Label*. In addition, AF Form 3227, **Privacy Act Cover Sheet**, is also available for use with PA material.

3.4.3.3. Before releasing personal information to a third party, ensure it is authorized, consider the consequences, and check its accuracy. You may release personal information to a third party when the subject agrees orally or in writing.

3.4.3.4. Dispose of records protected by the PA according to the records disposition schedules listed in AFMAN 37-139. Destroy these records by any method that prevents compromise (such as tearing, burning, or shredding) as long as the personal data is not recognizable and is beyond reconstruction.

3.4.3.5. The importance of these responsibilities is evident from the criminal penalties imposed by the PA on federal employees who violate certain sections of the law. For example, a fine of up to \$5,000 may be imposed for maintaining a PA system of record that has not been published in the *Federal Register* or for making an unauthorized disclosure. An injured party may also file a civil lawsuit against the Air Force.

### **3.5. Conditions of Disclosures to a Third Party:**

3.5.1. The no-disclosure-without-consent rule means you should never disclose information from a system of records by any means of communication, to any person or agency, except pursuant to a written request by, or with the prior written consent, of the individual to whom the record pertains.

3.5.2. There are 12 exceptions to the no-disclosure-without-consent rule. Disclosure under these exceptions are permissive, but not mandatory, as follows: (1) as a need to know within the agency, (2) as required under the FOIA, (3) for a routine use as published in the *Federal Register*, (4) to the Bureau of Census, (5) for statistical research, (6) to the National Archives, (7) for law enforcement purposes, (8)

for the health or safety of an individual, (9) to Congress, (10) to the General Accounting Office, (11) pursuant to a court order, and (12) to a consumer reporting agency in accordance with the Debt Collection Act.

3.5.3. Because disclosure of information from a system of records to a third party is a very complex process, always consult your PA Manager and AFI 33-332 *before* releasing records.

**3.6. Accounting for Disclosures.** The PA requires systems managers to keep an accurate record of all disclosures made from any system of records (except disclosures to DoD personnel for official use or under the FOIA). System managers may use AF Form 771, **Accounting of Disclosures**, for this purpose.

**3.7. Privacy and the Web.** Do not post personal information on publicly accessible DoD web sites unless clearly authorized by law and implementing directives or policy. Also, do not post personal information on nonpublicly accessible web sites unless the information is mission essential and appropriate safeguards have been established.

**3.8. Transmitting PA Information via E-mail.** For guidance on transmitting PA information via e-mail, contact your local information protection office or refer to the following instructions: AFI 33-201, *Communications Security (COMSEC) (FOUO)*; AFI 33-119, *Electronic Mail (E-Mail) Management and Use*; and AFI 33-129, *Transmission of Information via the Internet*.

**4. Summary.** Under the PA, each one of us has a responsibility to protect and safeguard an individual's personal information from unauthorized disclosures. Remember to protect someone else's information as if it were your own. As private citizens, the FOIA allows us to request copies of our own existing government records.

**5. Forms Adopted.** AF Forms 771 and 3227.

DAVID V. PULLIAM, Colonel, USAF  
Deputy Director of Communications and Information

### ***Attachment***

1. Glossary of References and Supporting Information

**Attachment 1****GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

*Federal Acquisition Regulation (FAR)*

*Federal Register*

*DoD 5400.7-R/AF Sup, DoD Freedom of Information Act Program*

*AFPD 37-1, Air Force Information Management (will become AFPD 33-3)*

*AFI 33-119, Electronic Mail (E-Mail) Management and Use*

*AFI 33-129, Transmission of Information via the Internet*

*AFI 33-201, Communications Security (COMSEC) (FOUO)*

*AFI 33-332, Air Force Privacy Act Program*

*AFMAN 37-139, Records Disposition Schedule (will become AFMAN 33-322, Volume 4)*

*AFVA 33-276, Air Force Privacy Act Label*

***Abbreviations and Acronyms***

**FOIA**—Freedom of Information Act

**FOUO**—for official use only

**PA**—Privacy Act