

**BY ORDER OF THE SECRETARY
OF THE AIR FORCE**

AIR FORCE INSTRUCTION 33-332

8 NOVEMBER 2000



**AIR FORCE SPACE COMMAND
Supplement 1**

1 JULY 2002

Communications and Information

AIR FORCE PRIVACY ACT PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: <http://afpubs.hq.af.mil>.

OPR: HQ USAF/SCTIR (Ms. Anne Rollins)

Certified by: HQ USAF/SCXX (Col T. G. Pricer)

Supersedes AFI 33-332, 12 October 1999

Pages: 47

AFI37-132_AFSPCSUP1, 2 Jan 97

Distribution: F

This instruction implements AFPD 37-1, *Air Force Information Management* (will convert to AFPD 33-3). It also implements Department of Defense (DoD) Directive 5400.11, *Department of Defense Privacy Program*, June 9, 1982, and DoD 5400.11-R, *Department of Defense Privacy Program*, August 1983. It sets guidelines for collecting, safeguarding, maintaining, using, accessing, amending and disseminating personal data kept in systems of records to comply with the Air Force Privacy Act Program. It takes precedence over any other instruction that deals with personal privacy and rights of individuals regarding their records. This instruction applies to the Air Force Reserve, Air National Guard, and those combatant commands where the Air Force is the executive agent. Use of the term "MAJCOM" through this instruction includes MAJCOMs, FOAs, and DRUs. Send all supplements to this instruction to Headquarters United States Air Force (HQ USAF/SCTIR), 1250 Air Force Pentagon, Washington DC 20330-1250. Send recommended changes or comments to Headquarters Air Force Communications Agency (HQ AFCA/ITPP), 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, through appropriate channels, using AF Form 847, **Recommendation for Change of Publication**, with an information copy to HQ USAF/SCTIR. Refer to **Attachment 1** for a glossary of references and supporting information.

This instruction requires collecting and maintaining information protected by the Privacy Act of 1974 authorized by Title 10, United States Code, Section 8013. System of Records notice F033 AF CIC C, Privacy Act Request File, applies. Maintain and dispose of records created as a result of processes prescribed by this AFI in accordance with AFMAN 37-139, *Records Disposition Schedule* (will convert to AFI 33-338).

(AFSPC) The OPR for this supplement is HQ AFSPC/SCXX (Mr. Terry J. Flesher). This supplement implements and extends the guidance of Air Force Instruction (AFI) 33-332, *Air Force Privacy Act Program*. The AFI is published word-for-word without editorial review. Air Force Space Command (AFSPC) supplemental material is indicated in bold face. This supplement describes

AFSPC's procedures for use in conjunction with the basic AFI. This supplement applies to HQ United States Space Command, HQ Air Force Space Command, subordinate units, and those agencies supported by HQ AFSPC. It does not apply to the Air Force Reserve or the Air National Guard units. Upon receipt of this integrated supplement, discard the Air Force basic publication.

SUMMARY OF REVISIONS

This change incorporates interim change (IC) 2000-1 (**Attachment 5**). It changes training requirements to comply with SecDef (A&M) memo of 9 June 2000, and HQ AFCIC/ITC office symbol to HQ USAF/SCTIR.

(AFSPC) Aligns guidance with AFI 33-332. Deletes requirement to generate annual Privacy Act report in accordance with Air Force direction.

AFI33-332 1 JULY 2002	3
Chapter 1— OVERVIEW OF THE PRIVACY ACT PROGRAM⁶	
1.1. Basic Guidelines	6
1.2. Violation Penalties	6
1.3. Personal Notes	7
1.4. Responsibilities	7
Chapter 2— OBTAINING LAW ENFORCEMENT RECORDS AND PROMISES OF CONFIDENTIALITY	9
2.1. Obtaining Law Enforcement Records	9
2.2. Promising Confidentiality	9
Chapter 3— COLLECTING PERSONAL INFORMATION	10
3.1. How To Collect Personal Information	10
3.2. When To Give Privacy Act Statements (PAS)	10
3.3. Requesting the SSN	10
Chapter 4— GIVING ACCESS TO PA RECORDS	12
4.1. Making a Request for Access	12
4.2. Processing a Request for Access	12
4.3. Fees	12
4.4. Denying or Limiting Access	13
4.5. Denial Authorities	13
Chapter 5— AMENDING THE RECORD	15
5.1. Amendment Reasons	15
5.2. Responding to Amendment Requests	15
5.3. Approving or Denying a Record Amendment	15
5.4. Seeking Review of Unfavorable Agency Determinations	15
5.5. Appeal Procedures	15
5.6. Contents of PA Case Files	16
Chapter 6— PA NOTIFICATIONS	17
6.1. When To Include a Privacy Act Warning Statement in Publications	17
6.2. Publishing System Notices	17
6.3. Submitting Notices for Publication in the	17
6.4. Reviewing Notices	17

Chapter 7— PROTECTING AND DISPOSING OF RECORDS	18
7.1. Protecting Records	18
7.2. Balancing Protection	18
7.3. Disposing of Records	18
Chapter 8— PA EXEMPTIONS	19
8.1. Requesting an Exemption	19
8.2. Exemption Types	19
8.3. Authorizing Exemptions	19
8.4. Approved Exemptions	19
Chapter 9— DISCLOSING RECORDS TO THIRD PARTIES	20
9.1. Disclosure Considerations	20
9.2. Disclosing Information for Which Consent Is Not Required	20
9.3. Disclosing Other Information	21
9.4. Agencies or Individuals to Whom the Air Force May Release Privacy In	21
9.5. Disclosing the Medical Records of Minors	22
9.6. Disclosure Accountings	22
9.7. Computer Matching	23
9.8. Privacy and the Web	23
Chapter 10— TRAINING	25
10.1. Who Needs Training	25
10.2. Training Tools	25
Chapter 11— PA REPORTING	26
11.1. Privacy Act Report (RCS: DD-DA&M[A]1379)	26
11.2. Information Collections, Forms, and Records.	26
Attachment 1— GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION	27
Attachment 2— PREPARING A SYSTEM NOTICE	31
A2.1. System Identification Number	31
A2.2. System Name.	31
A2.3. System Location.	31
A2.4. Categories of Individuals Covered by the System.	31

AFI33-332 1 JULY 2002	5
A2.5. Categories of Records in the System.	31
A2.6. Authority for Maintenance of the System.	31
A2.7. Purpose(s).	31
A2.8. Routine Uses of Records Maintained in the System Including Categories of	31
A2.9. Policies and Practices for Storing, Retrieving, Accessing, Retaining, and	31
A2.10. System Manager(s) and Address.	32
A2.11. Notification Procedure.	32
A2.12. Record Access Procedures.	32
A2.13. Contesting Records Procedures	32
A2.14. Record Source Categories.	32
A2.15. Exemptions Claimed for the System.	32
Attachment 3— GENERAL AND SPECIFIC EXEMPTIONS	33
A3.1. General Exemptions.	33
A3.2. Specific Exemptions.	33
Attachment 4— IC 99-1 TO AFI 37-132, AIR FORCE PRIVACY ACT PROGRAM	37
Attachment 5— IC 2000-1 TO AFI 33-332, AIR FORCE PRIVACY ACT PROGRAM	45

Chapter 1

OVERVIEW OF THE PRIVACY ACT PROGRAM

1.1. Basic Guidelines . The Privacy Act of 1974 and this instruction apply only to information in Air Force systems of records on living US citizens and permanent resident aliens.

1.1.1. An official system of records must be:

1.1.1.1. Authorized by law or Executive Order.

1.1.1.2. Controlled by an Air Force or lower level directive.

1.1.1.3. Needed to carry out an Air Force mission or function.

1.1.2. The Air Force does not:

1.1.2.1. Keep records on how a person exercises First Amendment rights. **EXCEPTIONS are when:** The Air Force has the permission of that individual or is authorized by federal statute; or the information pertains to an authorized law enforcement activity.

1.1.2.2. Penalize or harass an individual for exercising rights guaranteed under the Privacy Act. Give reasonable aid to individuals exercising their rights.

1.1.3. Air Force members:

1.1.3.1. Keep paper and electronic records containing personal information and retrieved by name or personal identifier only in approved systems published in the *Federal Register*.

1.1.3.2. Collect, maintain, and use information in such systems only to support programs authorized by law or Executive Order.

1.1.3.3. Safeguard the records in the system and keep them the minimum time required.

1.1.3.4. Keep the records timely, accurate, complete, and relevant.

1.1.3.5. Amend and correct records on request.

1.1.3.6. Let individuals review and receive copies of their own records unless the Secretary of the Air Force approved an exemption for the system or the Air Force created the records in anticipation of a civil action or proceeding.

1.1.3.7. Provide a review of decisions that deny individuals access to or amendment of their records.

1.2. Violation Penalties . An individual may file a civil suit against the Air Force for failing to comply with the Privacy Act. The courts may find an individual offender guilty of a misdemeanor and fine that individual offender not more than \$5,000 for:

1.2.1. Willfully maintaining a system of records that doesn't meet the public notice requirements.

1.2.2. Disclosing information from a system of records to someone not entitled to the information.

1.2.3. Obtaining someone else's records under false pretenses.

1.3. Personal Notes . If you keep personal notes on individuals to use as memory aids to supervise or perform other official functions, and do not share them with others, and an Air Force directive does not require their maintenance, the PA does not apply.

1.4. Responsibilities .

1.4.1. The Deputy Chief of Staff, Communications and Information (HQ USAF/SC), is the senior Air Force Privacy Official with overall responsibility for the Air Force Privacy Act Program.

1.4.2. The Office of the General Counsel to the Secretary of the Air Force (SAF/GCA) makes final decisions on appeals.

1.4.3. The Director, Architecture and Interoperability (HQ USAF/SCT), manages the program through the Air Force Privacy Act Office in the Information Dissemination and Management Division (HQ USAF/SCTIR), who:

1.4.3.1. Administers procedures outlined in this instruction.

1.4.3.2. Submits system notices and required reports to the Defense Privacy Office.

1.4.3.3. Guides major commands (MAJCOM) and field operating agencies (FOA).

1.4.4. MAJCOM and FOA commanders, HQ USAF and Deputy Chiefs of Staff (DCS), and comparable officials, and SAF offices implement this instruction. Each HQ USAF and SAF office appoints a PA monitor. Send the name, office symbol, and phone number to HQ USAF/SCTIR.

1.4.5. MAJCOMs:

1.4.5. (AFSPC) The Command Records Manager assigned to HQ AFSPC/SCXX is delegated responsibility as the Command Privacy Act Program Manager/Privacy Act Officer.

1.4.5.1. Manage the program.

1.4.5.2. Appoint a command PA officer.

1.4.5.3. Send the name, office symbol, and phone number to HQ USAF/SCTIR.

1.4.6. PA Officers:

1.4.6. (AFSPC) The installation commander appoints the installation/DRU Privacy Act Officer.

1.4.6.1. Guide and train.

1.4.6.2. Review the program at regular intervals.

1.4.6.3. Submit reports.

1.4.6.4. Review all publications and forms for compliance with this instruction.

1.4.6.5. Review system notices.

1.4.6.6. Investigate complaints.

1.4.6.7. Staff denial recommendations (at MAJCOMs and FOAs only).

1.4.7. System Managers:

1.4.7.1. Decide the need for, and content of systems.

1.4.7.2. Manage and safeguard the system.

- 1.4.7.3. Train personnel on PA requirements.
- 1.4.7.4. Protect records from unauthorized disclosure, alteration, or destruction.
- 1.4.7.5. Prepare system notices and reports.
- 1.4.7.6. Answer PA requests.
- 1.4.7.7. Keep records of disclosures.
- 1.4.7.8. Evaluate the systems annually.

1.4.8. PA Monitors (PAM):

1.4.8. (AFSPC) The Functional Area Records Manager (FARM) or Information Manager, as determined by installation/DRU Privacy Act Officer, is delegated as unit/staff PA monitor.

- 1.4.8.1. Are the focal point in their functional area for general PA questions and correspondence.
- 1.4.8.2. Maintain a list of all systems of records and system managers in their area.
- 1.4.8.3. Act as liaison with the PA Officer.
- 1.4.8.4. Maintain statistics for the annual Privacy Act report.

Chapter 2

OBTAINING LAW ENFORCEMENT RECORDS AND PROMISES OF CONFIDENTIALITY

2.1. Obtaining Law Enforcement Records . The Commander AFOSI; the Commander, Air Force Security Forces Center; MAJCOM, FOA, and base chiefs of security forces; AFOSI detachment commanders; and designees of those offices may ask another agency for records for law enforcement under 5 USC 552a(b)(7). The requesting office must indicate in writing the specific part of the record desired and identify the law enforcement activity asking for the record.

2.2. Promising Confidentiality . Record promises of confidentiality to exempt from disclosure any "confidential" information under subsection (k)(2), (k)(5), or (k)(7) of the Privacy Act.

Chapter 3

COLLECTING PERSONAL INFORMATION

3.1. How To Collect Personal Information . Collect personal information directly from the subject of the record when possible. You may ask third parties when:

- 3.1.1. You must verify information.
- 3.1.2. You want opinions or evaluations.
- 3.1.3. You can't contact the subject.
- 3.1.4. The subject asks you.

3.2. When To Give Privacy Act Statements (PAS) . Give a PAS orally or in writing: (1) to anyone from whom you are collecting personal information that will be put in a system of records; or (2) whenever you ask someone for his or her Social Security number (SSN). **NOTE:** Do this regardless of how you collect or record the answers. You may display a sign in areas where people routinely furnish this kind of information. Give a copy of the PAS if asked. Do not ask the person to sign the PAS.

3.2.1. A PAS must include four items:

- 3.2.1.1. Authority: The legal authority, that is, the United States Code or Executive Order authorizing the program the system supports.
- 3.2.1.2. Purpose: The reason you are collecting the information.
- 3.2.1.3. Routine Uses: A list of where and why the information will be disclosed outside DoD.
- 3.2.1.4. Disclosure: Voluntary or Mandatory. (Use Mandatory only when disclosure is required by law and the individual will be penalized for not providing information.) Include any consequences of nondisclosure in nonthreatening language.

3.3. Requesting the SSN . Do not deny people a legal right, benefit, or privilege for refusing to give their SSNs unless the law requires disclosure, or a law or regulation adopted before January 1, 1975 required the SSN and the Air Force uses it to verify a person's identity in a system of records established before that date. When you ask for an SSN to create a record, tell the individual: (1) the statute, regulation, or rule authorizing you to ask for the SSN; (2) the uses that will be made of the SSN; (3) if he or she is legally obligated to provide the SSN.

3.3.1. The Air Force requests an individual's SSN and provides the individual information required by law when anyone enters military service or becomes an Air Force civilian employee. The Air Force uses the SSN as a service or employment number to reference the individual's official records. When you ask someone for an SSN as identification (ID) to retrieve an existing record, you do not have to restate this information.

3.3.2. Executive Order 9397, November 22, 1943, authorizes using the SSN as a personal identifier. This order is not adequate authority to collect an SSN to create a record. When law does not require disclosing the SSN or when the system of records was created after January 1, 1975, you may ask for the SSN, but the individual does not have to disclose it. If the individual refuses to respond, use alternative means of identifying records.

3.3.3. SSNs are personal and unique to each individual. Protect them as FOR OFFICIAL USE ONLY (FOUO). Do not disclose them to anyone without an official need to know.

Chapter 4

GIVING ACCESS TO PA RECORDS

4.1. Making a Request for Access . Persons or their designated representatives may ask for a copy of their records in a system of records. Requesters need not state why they want access to their records. Verify the identity of the requester to avoid unauthorized disclosures. How you verify identity will depend on the sensitivity of the requested records. Persons without access to notary services may use an unsworn declaration in the following format: "I declare under penalty of perjury (if outside the United States, add "under the laws of the United States of America") that the foregoing is true and correct. Executed on (date). (Signature)."

4.2. Processing a Request for Access . Consider a request from an individual for his or her own records in a system of records under both the Freedom of Information Act (FOIA) and the PA regardless of the Act cited. The requester need not cite any Act. Process the request under whichever Act gives the most information. When necessary, tell the requester under which Act you processed the request and why.

4.2.1. Requesters should describe the records they want. They do not have to name a system of records number, but they should at least name a type of record or functional area. For requests that ask for "all records about me," ask for more information and tell the person how to review the Air Force systems of records published in the Federal Register or at <http://www.defenselink.mil/privacy/notices/usaf>.

4.2.2. Requesters should not use government equipment, supplies, stationery, postage, telephones, or official mail channels for making PA requests. PA Officers and system managers process such requests but tell requesters that using government resources to make PA requests is not authorized.

4.2.3. Tell the requester if a record exists and how to review the record. If possible, respond to requests within 10 workdays of receiving them. If you cannot answer the request in 10 workdays, send a letter explaining why and give an approximate completion date no more than 20 workdays after the first office received the request.

4.2.4. Show or give a copy of the record to the requester within 30 workdays of receiving the request unless the system is exempt and the Air Force lists the exemption in **Attachment 3**; 32 CFR 806b.13; or published as a final rule in the *Federal Register*. Give information in a form the requester can understand.

4.2.5. If the requester wants another person present during the record review, the system manager may ask for written consent to authorize discussing the record with another person present.

4.3. Fees . Give the first 100 pages free, and charge only reproduction costs for the remainder. Copies cost \$.15 per page; microfiche costs \$.25 per fiche. Charge the fee for the first 100 pages if records show that the Air Force already responded to a request for the same records at no charge. Do not charge fees:

4.3.1. When the requester can get the record without charge under another publication (for example, medical records).

4.3.2. For search.

4.3.3. For reproducing a document for the convenience of the Air Force.

4.3.4. For reproducing a record so the requester can review it.

4.4. Denying or Limiting Access . Process access denials within 5 workdays after you receive a request for access. When you may not release a record, send a copy of the request, the record, and why you recommend denying access (including the applicable exemption) to the denial authority through the Staff Judge Advocate (SJA) and the PA officer. The SJA gives a written legal opinion on the denial. The MAJ-COM or FOA PA officer reviews the file, gets written advice from the SJA and the functional office of primary responsibility (OPR), and makes a recommendation to the denial authority. The denial authority sends the requester a letter with the decision. If the denial authority grants access, release the record. If the denial authority refuses access, tell the requester why and explain pertinent appeal rights.

4.4.1. Before you deny a request for access to a record, make sure that:

4.4.1.1. The system has an exemption approved by HQ USAF/SCTIR (as listed in **Attachment 3**, 32 CFR 806b.13, or published as a final rule in the *Federal Register*).

4.4.1.2. The exemption covers each document. (All parts of a system are not automatically exempt.)

4.4.1.3. Nonexempt parts are segregated.

4.4.2. You may refuse to give out medical records if a physician believes that doing so could harm the person's mental or physical health. You have these options:

4.4.2.1. Ask the requester to get a letter from a physician to whom you can send the records. Include a letter explaining to the physician that giving the records directly to the individual could be harmful.

4.4.2.2. Offer the services of a military physician other than one who provided treatment if naming the physician poses a hardship on the individual.

4.4.3. Do not delete third-party information from a record when the subject requests access, except as noted in paragraph **4.4.4.**, unless the Air Force covers the record with an established exemption (Attachment 3, 32 CFR 806b.13, or published as a final rule in the *Federal Register*). Presume that all information in a file pertains to the subject of the file.

4.4.4. Do not release third-party personal data (such as SSN and home address). This action is not a denial.

4.4.5. Withhold records compiled in connection with a civil action or other proceeding including any action where the Air Force expects judicial or administrative adjudicatory proceedings. This exemption does not cover criminal actions. Do not release attorney work products prepared before, during, or after the action or proceeding.

4.5. Denial Authorities . These officials or a designee may deny access or amendment of records as authorized by the Privacy Act. Send a letter to HQ USAF/SCTIR with the position titles of designees. You must get HQ USAF/SCTIR approval before delegating this authority to a lower level. Send requests for waiver with justification to HQ USAF/SCTIR. Authorities are:

4.5.1. DCSs and chiefs of comparable offices or higher level at SAF or HQ USAF.

4.5.1. (Added) (AFSPC Only). The Staff Judge Advocate, HQ AFSPC, is designated as the Air Force Space Command denial authority.

4.5.2. MAJCOM or FOA commanders.

4.5.2. (Added) (USSPACECOM Only). The Joint Secretary, USSPACECOM, is designated as the United States Space Command denial authority.

4.5.3. HQ USAF/DPF, 1040 Air Force Pentagon, Washington DC 20330-1040 (for civilian personnel records).

4.5.4. Commander, Air Force Office of Special Investigations (AFOSI), Washington DC 20332-6001 (for AFOSI records).

Chapter 5

AMENDING THE RECORD

5.1. Amendment Reasons . Individuals may ask to have their records amended to make them accurate, timely, relevant, or complete. System managers routinely correct a record if the requester can show that it is factually wrong.

5.2. Responding to Amendment Requests .

5.2.1. Anyone may request minor corrections orally. Requests for more serious modifications should be in writing.

5.2.2. After verifying the identity of the requester, make the change, notify all known recipients of the record, and inform the individual.

5.2.3. Acknowledge requests within 10 workdays of receipt. Give an expected completion date unless you complete the change within that time. Final decisions must take no longer than 30 workdays.

5.3. Approving or Denying a Record Amendment . The Air Force does not usually amend a record when the change is based on opinion, interpretation, or subjective official judgment. This action constitutes a denial, and requesters may appeal. If the system manager decides not to amend or partially amend the record, send a copy of the request, the record, and the recommended denial reasons to the denial authority through the SJA and the PA officer. SJAs will include a legal opinion.

5.3.1. The MAJCOM or FOA PA officer reviews the proposed denial, gets a legal opinion from the SJA and written advice from the functional OPR, and makes a recommendation to the denial authority.

5.3.2. The denial authority sends the requester a letter with the decision. If the denial authority approves the request, amend the record and notify all previous recipients that it has been changed. If the authority denies the request, give the requester the statutory authority, reason, and pertinent appeal rights.

5.4. Seeking Review of Unfavorable Agency Determinations . Requesters should pursue record corrections of subjective matters and opinions through proper channels to the Civilian Personnel Office using grievance procedures or the Air Force Board for Correction of Military Records (AFBCMR). Record correction requests denied by the AFBCMR are not subject to further consideration under this instruction.

5.5. Appeal Procedures . Individuals may request a denial review by writing to the Secretary of the Air Force, through the denial authority, within 60 calendar days after receiving a denial letter. The denial authority promptly sends a complete appeal package to HQ USAF/SCTIR. The package must include: (1) the original appeal letter; (2) the initial request; (3) the initial denial; (4) a copy of the record; (5) any internal records or coordination actions relating to the denial; (6) the denial authority's comments on the appellant's arguments; and (7) the legal reviews.

5.5.1. If the denial authority reverses an earlier denial and grants access or amendment, notify the requester immediately.

5.5.2. HQ USAF/SCTIR reviews the denial and sends it to SAF/GCA through HQ USAF/JAG for legal review or staffing to grant or deny the appeal. SAF/GCA tells the requester the final Air Force decision and explains judicial review rights.

5.5.3. The requester may file a concise statement of disagreement with the system manager if SAF/GCA denies the request to amend the record. SAF/GCA explains the requester's rights when they issue the final appeal decision.

5.5.3.1. The records should clearly show that a statement of disagreement is filed with the record or separately.

5.5.3.2. The disputed part of the record must show that the requester filed a statement of disagreement.

5.5.3.3. Give copies of the statement of disagreement to the record's previous recipients. Inform subsequent record users about the dispute and give them a copy of the statement with the record.

5.5.3.4. The system manager may include a brief summary of the reasons for not amending the record. Limit the summary to the reasons SAF/GCA gave to the individual. The summary is part of the individual's record, but it is not subject to amendment procedures.

5.6. Contents of PA Case Files . Do not keep copies of disputed records in this file. Use the file solely for statistics and to process requests. Do not use the case files to make any kind of determination about an individual. Document reasons for untimely responses. These files include:

5.6.1. Requests from and replies to individuals on whether a system has records about them.

5.6.2. Requests for access or amendment.

5.6.3. Approvals, denials, appeals, and final review actions.

5.6.4. Coordination actions and related papers.

Chapter 6

PA NOTIFICATIONS

6.1. When To Include a Privacy Act Warning Statement in Publications . Include a Privacy Act Warning Statement in each Air Force publication that requires collecting or keeping personal information in a system of records. Also include the Warning Statement when publications direct collection of the SSN from the individual. The warning statement will cite legal authority and the system of records number and title. You can use the following warning statement: "This instruction requires collecting and maintaining information protected by the Privacy Act of 1974 authorized by (*U.S.C. citation and or Executive Order number*). System of records notice (*number and title*) applies."

6.2. 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. The PA also requires submission of new or significantly changed systems to the Office of Management and Budget (OMB) and both houses of the Congress before publication in the *Federal Register*. This includes:

- 6.2.1. Starting a new system.
- 6.2.2. Instituting significant changes to an existing system.
- 6.2.3. Sending out data collection forms or instructions.
- 6.2.4. Issuing a request for proposal or invitation for bid to support a new system.

6.3. Submitting Notices for Publication in the *Federal Register*. At least 120 days before implementing a new system subject to this instruction, system managers must send a proposed notice, through the MAJCOM Privacy Office, to HQ USAF/SCTIR. Send notices electronically to afstif@af.pentagon.mil using Microsoft Word. Mark changes to existing notices using the revision tool in Word. Follow format outlined in **Attachment 2**. On new systems, system managers must include a statement that a risk assessment was accomplished and is available should the OMB request it.

6.4. Reviewing Notices . System managers review their notices annually and submit changes to HQ USAF/SCTIR through the MAJCOM Privacy Office.

Chapter 7

PROTECTING AND DISPOSING OF RECORDS

7.1. Protecting Records . Protect information according to its sensitivity level. Consider the personal sensitivity of the information and the risk of loss or alteration. Most information in systems of records is FOR OFFICIAL USE ONLY (FOUO). Refer to AFI 37-131, *Air Force Freedom of Information Act Program*, for protection methods.

7.2. Balancing Protection . Balance additional protection against risk and cost. AF Form 3227, **Privacy Act Cover Sheet**, is available for use with Privacy Act material. For example, a password may be enough protection for an automated system with a log-on protocol. Classified computer systems or those with established audit and password systems are obviously less vulnerable than unprotected files or word processors in offices that are periodically empty. Follow AFI 33-202, *The Air Force Computer Security Program*, for procedures on safeguarding personal information in automated records.

7.3. Disposing of Records . You may use the following methods to dispose of records protected by the Privacy Act according to records retention schedules:

7.3.1. 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.

7.3.2. Degauss or overwrite magnetic tapes or other magnetic medium.

7.3.3. Dispose of paper products through the Defense Reutilization and Marketing Office (DR&MO) or through activities who manage a base-wide recycling program. 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 PA 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.

Chapter 8

PA EXEMPTIONS

8.1. Requesting an Exemption . A system manager who believes that a system needs an exemption from some or all of the requirements of the PA should send a request to HQ USAF/SCTIR through the MAJCOM or FOA PA Officer. The request should detail the reasons for the exemption, the section of the Act that allows the exemption, and the specific subsections of the PA from which the system is to be exempted, with justification for each subsection.

8.2. Exemption Types .

8.2.1. A *General exemption* frees a system from most parts of the PA.

8.2.2. A *Specific exemption* frees a system from only a few parts.

8.3. Authorizing Exemptions . Only HQ USAF/SCTIR can approve exempt systems of records from any part of the Privacy Act. Denial authorities can withhold records using these exemptions *only* if HQ USAF/SCTIR previously approved and published an exemption for the system in the *Federal Register*. **Attachment 3** lists the systems of records that have approved exemptions.

8.4. Approved Exemptions . Approved exemptions exist under 5 U.S.C. 552a for:

8.4.1. Certain systems of records used by activities whose principal function is criminal law enforcement (subsection [j][2]).

8.4.2. Classified information in any system of records (subsection[k][1]).

8.4.3. Law enforcement records (other than those covered by subsection [j][2]). 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) (subsection [k][2]).

8.4.4. Statistical records required by law. Data is for statistical use only and may not be used to decide individuals' rights, benefits, or entitlements (subsection[k][4]).

8.4.5. Data to determine suitability, eligibility, or qualifications for federal service or contracts, or access to classified information if access would reveal a confidential source (subsection [k][5]).

8.4.6. Qualification tests for appointment or promotion in the federal service if access to this information would compromise the objectivity of the tests (subsection [k][6]).

8.4.7. Information which the Armed Forces uses to evaluate potential for promotion if access to this information would reveal a confidential source (subsection [k][7]).

Chapter 9

DISCLOSING RECORDS TO THIRD PARTIES

9.1. Disclosure Considerations . Before releasing personal information to third parties, make sure it is authorized, consider the consequences, and check accuracy. You can release personal information to third parties when the subject agrees orally or in writing. Air Force members consent to releasing their home telephone number and address when they sign and check the "Do Consent" block on the AF Form 624, **Base/Unit Locator and PSC Directory** (see AFI 33-329, *Base and Unit Personnel Locators*).

9.1.1. Before including personal information such as home addresses, home phones, and similar information on social rosters or directories, ask for written consent statements. Otherwise, do not include the information.

9.1.2. You must get written consent before releasing any of these items of information. This list is not all inclusive:

9.1.2.1. Marital status.

9.1.2.2. Number and sex of dependents.

9.1.2.3. Civilian educational degrees and major areas of study (unless the request for the information relates to the professional qualifications for federal employment).

9.1.2.4. School and year of graduation.

9.1.2.5. Home of record.

9.1.2.6. Home address and phone.

9.1.2.7. Age and date of birth.

9.1.2.8. Present or future assignments for overseas or for routinely deployable or sensitive units.

9.1.2.9. Office and unit address and duty phone for overseas or for routinely deployable or sensitive units.

9.1.2.10. Race.

9.1.2.11. Educational level (unless the request for the information relates to the professional qualifications for federal employment).

9.2. Disclosing Information for Which Consent Is Not Required . You don't need consent before releasing any of these items:

9.2.1. Information releasable under the FOIA.

9.2.2. Information for use within DoD by officials or employees with a need to know.

9.2.3. Name.

9.2.4. Rank.

9.2.5. Grade.

9.2.6. Air Force specialty code (AFSC).

- 9.2.7. Pay (including base pay, special pay, all allowances except Basic Allowance for Quarters [BAQ] and Variable Housing Allowance [VHA]).
- 9.2.8. Gross salary for civilians.
- 9.2.9. Past duty assignments.
- 9.2.10. Present and future approved and announced stateside assignments.
- 9.2.11. Position title.
- 9.2.12. Office, unit address, and duty phone number.
- 9.2.13. Date of rank.
- 9.2.14. Entered on active duty (EAD) date.
- 9.2.15. Pay date.
- 9.2.16. Source of commission.
- 9.2.17. Professional military education.
- 9.2.18. Promotion sequence number.
- 9.2.19. Military awards and decorations.
- 9.2.20. Duty status of active, retired, or reserve.
- 9.2.21. Active duty official attendance at technical, scientific, or professional meetings.
- 9.2.22. Biographies and photos of key personnel.
- 9.2.23. (Added) (AFSPC) Consent is not required to release Date of Separation (DOS).**

9.3. Disclosing Other Information . Use these guidelines to decide whether to release information:

- 9.3.1. Would the subject have a reasonable expectation of privacy in the information requested?
- 9.3.2. Would disclosing the information benefit the general public? The Air Force considers information as meeting the public interest standard if it reveals anything regarding the operations or activities of the agency, or performance of its statutory duties.
- 9.3.3. Balance the public interest against the individual's probable loss of privacy. Do *not* consider the requester's purpose, circumstances, or proposed use.

9.4. Agencies or Individuals to Whom the Air Force May Release Privacy Information. The Air Force may release information without consent to these individuals or agencies:

- 9.4.1. Agencies outside DoD for a Routine Use published in the *Federal Register*. The purpose of the disclosure must be compatible with the purpose in the Routine Use. When initially collecting the information from the subject, the Routine Uses block in the Privacy Act Statement must name the agencies and reason.
- 9.4.2. The Bureau of the Census to plan or carry out a census or survey under Title 13, U.S.C. Section 8.
- 9.4.3. A recipient for statistical research or reporting. The recipient must give advanced written assurance that the information is for statistical purposes only. **NOTE:** No one may use any part of the

record to decide on individuals' rights, benefits, or entitlements. You must release records in a format that makes it impossible to identify the real subjects.

9.4.4. The Archivist of the United States and the National Archives and Records Administration (NARA) to evaluate records for permanent retention. Records stored in Federal Records Centers remain under Air Force control.

9.4.5. A federal, state, or local agency (other than DoD) for civil or criminal law enforcement. The head of the agency or a designee must send a written request to the system manager specifying the record or part needed and the law enforcement purpose. The system manager may also disclose a record to a law enforcement agency if the agency suspects a criminal violation. This disclosure is a Routine Use for all Air Force systems of records and is published in the *Federal Register*.

9.4.6. An individual or agency that needs the information for compelling health or safety reasons. The affected individual need not be the record subject.

9.4.7. The Congress, a congressional committee, or a subcommittee, for matters within their jurisdictions.

9.4.8. A congressional office acting for the record subject. A published, blanket Routine Use permits this disclosure. If the material for release is sensitive, get a release statement.

9.4.9. The Comptroller General or an authorized representative of the General Accounting Office on business.

9.4.10. A court order of a court of competent jurisdiction, signed by a judge.

9.4.11. A consumer credit agency according to the Debt Collections Act when a published system notice lists this disclosure as a Routine Use.

9.4.12. A contractor operating a system of records under an Air Force contract. Records maintained by the contractor for the management of contractor employees are not subject to the PA.

9.5. Disclosing the Medical Records of Minors . Air Force personnel may disclose the medical records of minors to their parents or legal guardians. The laws of each state define the age of majority.

9.5.1. The Air Force must obey state laws protecting medical records of drug or alcohol abuse treatment, abortion, and birth control. If you manage medical records, learn the local laws and coordinate proposed local policies with the servicing SJA.

9.5.2. Outside the United States (overseas), the age of majority is 18. Unless parents or guardians have a court order granting access or the minor's written consent, they will not have access to minor's medical records overseas when the minor sought or consented to treatment between the ages of 15 and 17 in a program where regulation or statute provides confidentiality of records and he or she asked for confidentiality.

9.6. Disclosure Accountings . System managers must keep an accurate record of all disclosures made from any system of records except disclosures to DoD personnel for official use or disclosures under the FOIA. System managers may use AF Form 771, **Accounting of Disclosures**.

9.6. (AFSPC) If AF Form 771, Accounting of Disclosures, is not used, disclosed information is recorded in a format that can later be reconstructed to identify accounting of disclosure.

9.6.1. System managers may file the accounting record any way they want as long as they give it to the subject on request, send corrected or disputed information to previous record recipients, explain any disclosures, and provide an audit trail for reviews. Include in each accounting:

- 9.6.1.1. Release date.
- 9.6.1.2. Description of information.
- 9.6.1.3. Reason for release.
- 9.6.1.4. Name and address of recipient.

9.6.2. Some exempt systems let you withhold the accounting record from the subject.

9.6.3. You may withhold information about disclosure accountings for law enforcement purposes at the law enforcement agency's request.

9.7. Computer Matching . Computer matching programs electronically compare records from two or more automated systems which may include DoD, another federal agency, or a state or other local government. A system manager proposing a match that could result in an adverse action against a federal employee must meet these requirements of the PA: (1) prepare a written agreement between participants; (2) secure approval of the Defense Data Integrity Board; (3) publish a matching notice in the *Federal Register* before matching begins; (4) ensure full investigation and due process; and (5) act on the information, as necessary.

9.7.1. The PA applies to matching programs that use records from: federal personnel or payroll systems and federal benefit programs where matching: (1) determines federal benefit eligibility; (2) checks on compliance with benefit program requirements; (3) recovers improper payments or delinquent debts from current or former beneficiaries.

9.7.2. Matches used for statistics, pilot programs, law enforcement, tax administration, routine administration, background checks and foreign counterintelligence, and internal matching that won't cause any adverse action are exempt from PA matching requirements.

9.7.3. Any activity that expects to participate in a matching program must contact HQ USAF/SCTIR immediately. System managers must prepare a notice for publication in the *Federal Register* with a Routine Use that allows disclosing the information for use in a matching program. Send the proposed system notice to HQ USAF/SCTIR. Allow 180 days for processing requests for a new matching program.

9.7.3. (AFSPC) Any activity that expects to participate in a computer matching program must go through appropriate records management channels to HQ AFSPC/SCXX.

9.7.4. Record subjects must receive prior notice of a match. The best way to do this is to include notice in the Privacy Act Statement on forms used in applying for benefits. Coordinate computer matching statements on forms with HQ USAF/SCTIR through the MAJCOM PA Officer.

9.7.4. (AFSPC) Coordinate computer matching statements on forms through appropriate local Privacy Act Officers to HQ AFSPC/SCXX.

9.8. Privacy and the Web . Do not post personal information on publicly accessible DoD web sites unless clearly authorized by law and implementing regulation and policy. Additionally, do not post per-

sonal information on non-publicly accessible web sites unless it is mission essential and appropriate safeguards have been established. See AFIs 33-129 and 35-205.

Chapter 10

TRAINING

10.1. Who Needs Training . The Privacy Act requires training for all persons involved in the design, development, operation and maintenance of any system of records. More specialized training is needed for personnel who may be expected to deal with the news media or the public, personnel specialists, finance officers, information managers, supervisors, and individuals working with medical and security records. Commanders will ensure that above personnel are trained annually in the principles and requirements of the Privacy Act.

10.2. Training Tools . Helpful aids include:

10.2.1. "The Privacy Act of 1974," a 32-minute film developed by the Defense Privacy Office. Consult your local audiovisual library.

10.2.2. A Manager's Overview, *What You Need to Know About the Privacy Act*. This overview is available on-line at <http://www.foia.af.mil>.

NOTE:

Formal school training groups that develop or modify blocks of instruction must send the material to HQ USAF/SCTIR for coordination.

Chapter 11

PA REPORTING

11.1. Privacy Act Report (RCS: DD-DA&M[A]1379) . By 1 March of each year, MAJCOM and FOA PA officers must send HQ USAF/SCTIR a report covering the previous calendar year. The report includes:

- 11.1.1. Total number of written requests for access that cite the PA or FOIA which are processed under this instruction.
- 11.1.2. Total number of requests wholly or partially granted.
- 11.1.3. Total number of requests denied and the PA exemptions used.
- 11.1.4. Total number of requests for which no record was found.
- 11.1.5. Total number of requests to amend records.
- 11.1.6. Total number of amendment requests wholly or partially granted.
- 11.1.7. Total number of amendment requests denied.
- 11.1.8. Specific recommendations for changes to the Act or the PA Program.

11.2. Information Collections, Forms, and Records.

- 11.2.1. RCS: DD-DA&M[A]1379, Privacy Act Report, is mandated by this publication. See paragraph **11.1.** for guidance.
- 11.2.2. The following forms are prescribed by this publication: AF Form 3227, **Privacy Act Cover Sheet** and AF Form 771, **Accounting of Disclosures**.
- 11.2.3. Retain and dispose of Privacy Act records according to AFI 37-139, *Records Disposition Schedule* (will convert to AFI 33-322, Vol. 4), Table 37-1, using the appropriate rule.

WILLIAM J. DONAHUE, Lt Gen, USAF
Director, Communications and Information

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

Title 5, United States Code, Section 552a, as amended, *The Privacy Act of 1974*

Title 10, United States Code, Section 8013 *Secretary of the Air Force*

Executive Order 9397, *Numbering System for Federal Accounts Relating to Individual Persons*

32 Code of Federal Regulations 806b, *Air Force Privacy Act Program*

DoD Directive 5400.11, *Department of Defense Privacy Program*, June 9, 1982

DoD 5400.11-R, *Department of Defense Privacy Program*, August 1983

AFI 33-202, *Computer Security*

AFI 33-329, *Base and Unit Personnel Locators*

AFPD 37-1, *Air Force Information Management*

AFI 37-131, *Freedom of Information Act Program*

AFMAN 37-139, *Records Disposition Schedule* (will convert to AFI 33-338)

Abbreviations and Acronyms

AETC—Air Education and Training Command

AFA—Air Force Academy

AFBCMR—Air Force Board for Correction of Military Records

AFISA—Air Force Intelligence Services Agency

AFMC—Air Force Materiel Command

AFOSI—Air Force Office of Special Investigations

AFSC—Air Force Specialty Code

AFSCO—Air Force Security Clearance Office

AFSPA—Air Force Security Police Agency

ASCII—American Standard Code for Information Interchange

BAQ—Basic Allowance for Quarters

CFR—Code of Federal Regulations

DCS—Deputy Chief of Staff

DoD—Department of Defense

DR&MO—Defense Reutilization and Marketing Office

EAD—Entered on Active Duty

FOA—Field Operating Agency

FOIA—Freedom of Information Act

FOUO—For Official Use Only

IG—Inspector General

IMC—Interim Message Change

LE—Logistics and Engineering

MAJCOM—Major Command

MIRS—Management Information and Research System

MP—Military Personnel

MPC—Military Personnel Center

NARA—National Archives and Records Administration

OMB—Office of Management and Budget

OPM—Office of Personnel Management

OPR—Office of Primary Responsibility

PA—Privacy Act

PAM—Privacy Act Monitor

PAS—Privacy Act Statement

RCS—Reports Control Symbol

SAF—Secretary of the Air Force

SAF/GCA—Deputy General Counsel for Fiscal, Ethics, and Civilian Personnel

SG—Surgeon General

SJA—Staff Judge Advocate

SP—Security Police

SSN—Social Security Number

US—United States

USAF—United States Air Force

U.S.C.—United States Code

VHA—Variable Housing Allowance

Terms

Access—Allowing individuals to review or receive copies of their records.

Amendment—The process of adding, deleting, or changing information in a system of records to make the data accurate, relevant, timely, or complete.

Computer Matching—A computerized comparison of two or more automated systems of records or a system of records with non-Federal records to establish or verify eligibility for payments under Federal benefit programs or to recover delinquent debts for these programs.

Confidential Source—A person or organization giving information under an express or implied promise of confidentiality made before September 27, 1975.

Confidentiality—An expressed and recorded promise to withhold the identity of a source or the information provided by a source. The Air Force promises confidentiality only when the information goes into a system with an approved exemption for protecting the identity of confidential sources.

Defense Data Integrity Board—Representatives from the Services and DoD who oversee, coordinate, and approve all DoD computer matching programs covered by the Act.

Denial Authority—The individuals with authority to deny requests for access or amendment of records under the Privacy Act.

Disclosure—Giving information from a system, by any means, to anyone other than the record subject.

Federal Benefit Program—A federally funded or administered program for individuals that provides cash or in-kind assistance (payments, grants, loans, or loan guarantees).

Individual—A living US citizen or a permanent resident alien.

Matching Agency—The agency that performs a computer match.

Minor—Anyone under the age of majority according to local state law. If there is no applicable state law, a minor is anyone under age 18. Military members and married persons are not minors, no matter what their chronological age.

Personal Identifier—A name, number, or symbol which is unique to an individual, usually the person's name or SSN.

Personal Information—Information about an individual other than items of public record.

Privacy Act Request—An oral or written request by an individual about his or her records in a system of records.

Recipient Agency—An agency or contractor that receives the records and actually performs the computer match.

Record—Any information about an individual.

Routine Use—A disclosure of records to individuals or agencies outside DoD for a use that is compatible with the purpose for which the Air Force created the records.

Source Agency—A federal, state, or local government agency that discloses records for the purpose of a computer match.

System Manager—The official who is responsible for managing a system of records, including policies and procedures to operate and safeguard it. Local system managers operate record systems or are responsible for part of a decentralized system.

System of Records—A group of records containing personal information retrieved by the subject's name, personal identifier, or individual identifier through a cross-reference system.

System Notice—The official public notice published in the *Federal Register* of the existence and content

of the system of records.

Attachment 2

PREPARING A SYSTEM NOTICE

The following elements comprise a system of records notice for publication in the *Federal Register*:

A2.1. System Identification Number . HQ USAF/SCTIR assigns the notice number, for example, F033 AF PC A, where “F” indicates “Air Force,” the next number represents the series from AFMAN 37-139 (will convert to AFI 33-322, Vol. 4) regarding records disposition, and the final letter group shows the system manager’s command or DCS. The last character “A” indicates that this is the first notice for this series and system manager.

A2.2. System Name. Use a short, specific, plain-language title that identifies the system's general purpose (limited to 55 characters).

A2.3. System Location. Specify the address of the primary system and any decentralized elements, including automated data systems with a central computer facility and input or output terminals at separate locations. Use street address, 2-letter state abbreviations and 9-digit ZIP Codes. Spell out office names. Do not use office symbols.

A2.4. Categories of Individuals Covered by the System. Use nontechnical, specific categories of individuals about whom the Air Force keeps records. Do not use categories like "all Air Force personnel" unless they are actually true.

A2.5. Categories of Records in the System. Describe in clear, nontechnical terms, all categories of records in the system. List only documents actually kept in the system. Do not show source documents that are used to collect data and then destroyed. Do not list form numbers.

A2.6. Authority for Maintenance of the System. Cite the specific law or Executive Order that authorizes the program the records support. Cite the DoD directive or instruction or the Air Force or other instruction that authorizes the system of records. Always include titles with the citations. **NOTE:** Executive Order 9397 authorizes using the Social Security Number (SSN). Include this authority whenever the SSN is used to retrieve records.

A2.7. Purpose(s). Describe briefly and specifically what the Air Force does with the information collected.

A2.8. Routine Uses of Records Maintained in the System Including Categories of Users and the Purpose of Such Uses. The Blanket Routine Uses published in the Air Force Directory of System Notices apply to all system notices unless you indicate otherwise. Also list each specific agency or activity outside DoD to whom the records may be released and the purpose for such release.

A2.9. Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

A2.9.1. Storage. State the medium in which the Air Force keeps the records, for example, in file folders, card files, microfiche, computer, and so on. Storage does not refer to the storage container.

A2.9.2. Retrievability. State how the Air Force retrieves the records, for example, by name, SSN, or personal characteristics (such as fingerprints or voiceprints).

A2.9.3. Safeguards. List the kinds of officials who have immediate access to the system. List those responsible for safeguarding the records. Identify the system safeguards, for example, storage in safes, vaults, locked cabinets or rooms, use of guards, visitor controls, personnel screening, computer systems software, and so on. Describe safeguards fully without compromising system security.

A2.9.4. Retention and Disposal. State how long AFMAN 37-139 requires the activity to maintain the record. Indicate when or if the records may be transferred to a Federal Records Center and how long the record stays there. Specify when the Records Center sends the record to the National Archives or destroys it. Indicate how the records may be destroyed.

A2.10. System Manager(s) and Address. List the title and duty address of the system manager. For decentralized systems, show the locations and the position or duty title of each category of officials responsible for any segment of the system.

A2.11. Notification Procedure. List the title and duty address of the official authorized to tell requesters if their records are in the system. Specify the information a requester must submit, for example., full name, military status, SSN, date of birth, or proof of identity, and so on.

A2.12. Record Access Procedures. Explain how individuals may arrange to access their records. Include the titles or categories of officials who may assist, for example., the system manager.

A2.13. Contesting Records Procedures . HQ USAF/SCTIR provides this standard caption.

A2.14. Record Source Categories. Show categories of individuals or other information sources for the system. Do not list confidential sources protected by subsections (k)(2), (k)(5), or (k)(7) of the Act.

A2.15. Exemptions Claimed for the System. When a system has no approved exemption, write "none" under this heading. Specifically list any approved exemption including the subsection in the Act.

Attachment 3**GENERAL AND SPECIFIC EXEMPTIONS**

The Office of the Secretary of the Air Force has approved exemptions for the systems below:

A3.1. General Exemptions. The following systems of records have an approved (j)(2) exemption under 5 U.S.C. 552a:

A3.1.1. Counter Intelligence Operations and Collection Records, F124 AF A.

A3.1.2. Criminal Records, F124 AF C.

A3.1.3. Security Police Automated System (SPAS), F125 AF SP E.

A3.1.4. Investigative Support Records, F124 AF D.

A3.1.5. Correction and Rehabilitation Records, F125 AF A.

A3.1.6. Management Information and Research System (MIRS), F125 AF SP C (Exemption applies only for the period the individual is confined or in rehabilitation at an Air Force or federal correctional facility.).

A3.2. Specific Exemptions. The following systems of records have approved exemptions from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), (I), and (f) of 5 U.S.C. 552a:

A3.2.1. Classified Records:

A3.2.1.1. Exemption. All records in any system of records that are properly classified according to Executive Order are exempt regardless of whether the entire system is otherwise exempt.

A3.2.1.2. Authority. 5 U.S.C. 552a(k)(1).

A3.2.2. Admissions Records (F053 AFA C):

A3.2.2.1. Exemption. Parts of this system are exempt to the extent that disclosure would reveal a confidential source.

A3.2.2.2. Authority. 5 U.S.C. 552a(k)(7).

A3.2.2.3. Reasons. To ensure the frankness of information used to determine whether cadets are qualified for graduation and commissioning as officers in the Air Force.

A3.2.3. Air Force Personnel Test 851, Test Answer Cards (F035 MPC R):

A3.2.3.1. Exemption. This system is exempt.

A3.2.3.2. Authority. 5 U.S.C. 552a(k)(6).

A3.2.3.3. Reasons. To protect the objectivity of the promotion testing system by keeping the test questions and answers in confidence.

A3.2.4. Cadet Personnel Management System (F035 AFA A):

A3.2.4.1. Exemption. Parts of this system are exempt to the extent that disclosure would reveal the identity of a confidential source.

A3.2.4.2. Authority. 5 U.S.C. 552a(k)(7).

A3.2.4.3. Reasons. To maintain the candor and integrity of comments needed to evaluate an Air Force Academy cadet for commissioning in the Air Force.

A3.2.5. Cadet Records (F045 AETC C):

A3.2.5.1. Exemption. Parts of this system are exempt to the extent that disclosure would reveal the identity of a confidential source.

A3.2.5.2. Authority. 5 U.S.C 552a(k)(5).

A3.2.5.3. Reasons. To protect the identity of a confidential source who furnishes information necessary to make determinations about the qualification, eligibility, and suitability of cadets for graduation and commissioning in the Air Force.

A3.2.6. Family Advocacy Program Record (F168 AF SG B):

A3.2.6.1. Exemption. Parts of this system are exempt.

A3.2.6.2. Authority. 5 U.S.C 552a(k)(2) and (5).

A3.2.6.3. Reasons. To encourage those who know of exceptional medical or educational conditions or family maltreatment to come forward by protecting their identities and the integrity of ongoing and civil law investigations of criminal and civil law violations. Giving subjects access to their files could result in them concealing, altering, or fabricating evidence; could hamper the identification of offenders and alleged offenders; and could jeopardize the safety and well-being of the family.

A3.2.7. Effectiveness/Performance Reporting Systems (F035 AF MP A):

A3.2.7.1. Exemption. Brigadier General Selectee Effectiveness Reports and Colonel and Lieutenant Colonel Promotion Recommendations with close out dates on or before January 31, 1991, are exempt.

A3.2.7.2. Authority. 5 U.S.C. 552a(k)(7).

A3.2.7.3. Reasons. To ensure that selection boards have candid evaluations of officers being considered for promotion.

A3.2.8. Equal Opportunity in Off Base Housing (F030 AF LE A):

A3.2.8.1. Exemption. Parts of this system are exempt.

A3.2.8.2. Authority. 5 U.S.C. 552a(k)(2).

A3.2.8.3. Reasons. To enforce civil laws, court orders, and the activities of the Departments of Housing and Urban Development and Justice.

A3.2.9. Files on General Officers and Colonels Assigned to General Officer Positions (F035 MP A):

A3.2.9.1. Exemption. This system is exempt to the extent that disclosure would reveal the identity of a confidential source.

A3.2.9.2. Authority. 5 U.S.C. 552a(k)(7).

A3.2.9.3. Reasons. To protect the integrity of information used in the Reserve Initial Brigadier General Screening Board, the release of which would compromise the selection process.

A3.2.10. General Officer Personnel Data System (F035 AF MP P):

A3.2.10.1. Exemption. Air Force General Officer Promotion and Effectiveness Reports with close out dates on or before January 31, 1991, are exempt.

A3.2.10.2. Authority. 5 U.S.C. 552a(k)(7).

A3.2.10.3. Reasons. To ensure selection boards get candid evaluations of officers being considered for promotion to Major General, Lieutenant General, and General.

A3.2.11. Historical Airman Promotion Master Test File (F035 MPC L):

A3.2.11.1. Exemption. This system is exempt.

A3.2.11.2. Authority. 5 U.S.C. 552a(k)(6).

A3.2.11.3. Reasons. To protect the integrity, objectivity, and equity of the promotion testing system by keeping test questions and answers in confidence.

A3.2.12. Inspector General Records (F120 AF IG B):

A3.2.12.1. Exemption. Parts of this system are exempt unless a person is denied any right, privilege, or benefit, he or she would otherwise be entitled to as a result of keeping this material, then it must be released, unless doing so would reveal the identity of a confidential source.

A3.2.12.2. Authority. 5 U.S.C. 552a(k)(2).

A3.2.12.3. Reasons. Granting individuals access to information collected while an Inspector General inquiry is in progress could interfere with the just, thorough, and timely resolution of the complaint or inquiry and could possibly enable individuals to conceal wrong doing or mislead the inquiring officer. Disclosure might also subject sources, witnesses, and their families to harassment or intimidation.

A3.2.13. Investigative Applicant Processing Records (F124 AFOSI B):

A3.2.13.1. Exemption. This system is exempt to the extent that disclosure would reveal the identity of a confidential source.

A3.2.13.2. Authority. 5 U.S.C. 552a(k)(5).

A3.2.13.3. Reasons. To protect those who gave information in confidence during Air Force Office of Special Investigations (AFOSI) applicant inquiries. Fear of harassment could cause sources not to make frank and open responses about applicant qualifications. This could compromise the integrity of the AFOSI personnel program that relies on selecting only qualified people.

A3.2.14. Master Cadet Personnel Record (Active/Historical) (F035 AFA B):

A3.2.14.1. Exemption. Parts of this system are exempt to the extent that they would reveal the identity of a confidential source.

A3.2.14.2. Authority. 5 U.S.C. 552a(k)(7).

A3.2.14.3. Reasons. To maintain the candor and integrity of comments needed to evaluate a cadet for commissioning in the Air Force.

A3.2.15. Sensitive Compartmented Information Personnel Records (F205 AFISA A):

A3.2.15.1. Exemption. This system is exempt to the extent that disclosure would reveal the identity of a confidential source.

A3.2.15.2. Authority. 5 U.S.C. 552a(k)(2) and (k)(5).

A3.2.15.3. Reasons. To protect the identity of people promised confidentiality during investigations. Without these promises, sources will often be unwilling to provide information essential in adjudicating access in a fair and impartial manner.

A3.2.16. Security and Related Investigative Records (F124 AF B):

A3.2.16.1. Exemption. This system is exempt to the extent that disclosure would reveal the identity of a confidential source.

A3.2.16.2. Authority. 5 U.S.C. 552a(k)(5).

A3.2.16.3. Reasons. To protect the identity of those who give information in confidence for personnel security and related investigations; to protect sources against fear of harassment so they can give information in a frank and open way so investigators can pinpoint areas in an investigation that should be expanded to resolve charges of questionable conduct.

A3.2.17. Special Security Case Files (F205 AFSCO A):

A3.2.17.1. Exemption. This system is exempt to the extent that disclosure would reveal the identity of a confidential source.

A3.2.17.2. Authority. 5 U.S.C. 552a(k)(5).

A3.2.17.3. Reasons. To protect the identity of those who give information in confidence for personnel security and related investigations; to protect sources against fear of harassment so they can give information in a frank and open way so investigators can pinpoint areas in an investigation that should be expanded to resolve charges of questionable conduct.

A3.2.18. Special Security Files (F205 AF SP A):

A3.2.18.1. Exemption. This system is exempt to the extent that disclosure would reveal the identity of a confidential source.

A3.2.18.2. Authority. 5 U.S.C. 552a(k)(5).

A3.2.18.3. Reasons. To protect the identity of those who give information in confidence for personnel security and related investigations; to protect sources against fear of harassment so they can give information in a frank and open way so investigators can pinpoint areas in an investigation that should be expanded to resolve charges of questionable conduct.

A3.2.19. Application for Appointment and Extended Active Duty Files (F035 AF MP R):

A3.2.19.1. Exemption. This system is exempt to the extent that disclosure would reveal the identity of a confidential source.

A3.2.19.2. Authority. 5 U.S.C. 552a(k)(5).

A3.2.19.3. Reasons. To protect the identity of confidential sources who furnish information about the qualifications, eligibility, and suitability of health care professionals applying for Reserve of the Air Force appointment or interservice transfer to the Air Force.

Attachment 4**IC 99-1 TO AFI 37-132, AIR FORCE PRIVACY ACT PROGRAM****AIR FORCE INSTRUCTION 33-332**

12 OCTOBER 1999

Communications and Information

This instruction implements AFPD 37-1, *Air Force Information Management* (will convert to AFPD 33-3). It also implements Department of Defense (DoD) Directive 5400.11, *Department of Defense Privacy Program*, June 9, 1982, and DoD 5400.11-R, *Department of Defense Privacy Program*, August 1983. It sets guidelines for collecting, safeguarding, maintaining, using, accessing, amending and disseminating personal data kept in systems of records to comply with the Air Force Privacy Act Program. It takes precedence over any other instruction that deals with personal privacy and rights of individuals regarding their records. This instruction applies to the Air Force Reserve, Air National Guard, and those combatant commands where the Air Force is the executive agent. Use of the term "MAJCOM" through this instruction includes MAJCOMs, FOAs, and DRUs. Send all supplements to this instruction to HQ AFCIC/ITC, 1250 Air Force Pentagon, Washington DC 20330-1250. Send recommended changes or comments to HQ AFCA/XPPX, 203 W. Losey Street, Room 1060, Scott AFB IL 62225-5222, through appropriate channels, using AF Form 847, **Recommendation for Change of Publication**, with an information copy to HQ AFCIC/ITC. Refer to **Attachment 1** for a glossary of references and supporting information.

This instruction requires collecting and maintaining information protected by the Privacy Act of 1974 authorized by Title 10, United States Code, Section 8013. System of Records notice F033 AF CIC C, Privacy Act Request File, applies. Maintain and dispose of records created as a result of processes prescribed by this AFI in accordance with AFMAN 37-139, *Records Disposition Schedule* (will convert to AFI 33-338).

SUMMARY OF REVISIONS

This change incorporates interim change (IC) 99-1 (**Attachment 4**). This change converts the number of this instruction from AFI 37-132 to AFI 33-332. It reflects organizational changes; clarifies applicability; adds two categories of information normally not releasable without a person's consent; changes system notice submission procedures; adds requirement for risk assessment for new systems; adds requirement for annual review of systems by owners; and adds a new paragraph regarding posting personal information on the web; and clarifies reportable requests. A star (H) indicates revisions from previous edition.

1.4.1. The Director, Communications and Information (HQ USAF/SC) is the senior Air Force Privacy Official with overall responsibility for the Air Force Privacy Act program.

1.4.3. The Director, Chief Information Office manages the program through the Air Force Privacy Act Office in the Corporate Information Division (HQ AFCIC/ITC), who:

1.4.4. MAJCOM and FOA commanders, HQ USAF and Deputy Chiefs of Staff (DCS), and comparable officials, and SAF offices implement this instruction. Each HQ USAF and SAF office appoints a PA monitor. Send the name, office symbol, and phone number to HQ AFCIC/ITC.

1.4.5. MAJCOMs:

1.4.5.1. Manage the program.

1.4.5.2. Appoint a command PA officer.

1.4.5.3. Send the name, office symbol, and phone number to HQ AFCIC/ITC.

2.1. Obtaining Law Enforcement Records. The Commander AFOSI; the Commander, Air Force Security Forces Center; MAJCOM, FOA, and base chiefs of security forces; AFOSI detachment commanders; and designees of those offices may ask another agency for records for law enforcement under 5 USC 552a(b)(7). The requesting office must indicate in writing the specific part of the record desired and identify the law enforcement activity asking for the record.

4.2.1. Requesters should describe the records they want. They do not have to name a system of records number, but they should at least name a type of record or functional area. For requests that ask for "all records about me," ask for more information and tell the person how to review the Air Force systems of records published in the Federal Register or at <http://www.defenselink.mil/privacy/notices/usaf>.

4.4.1. Before you deny a request for access to a record, make sure that:

4.4.1.1. The system has an exemption approved by HQ AFCIC/ITC (as listed in Attachment 3, 32 CFR 806b.13, or published as a final rule in the *Federal Register*).

4.4.1.2. The exemption covers each document. (All parts of a system are not automatically exempt.)

4.4.1.3. Nonexempt parts are segregated.

4.5. Denial Authorities. These officials or a designee may deny access or amendment of records as authorized by the Privacy Act. Send a letter to HQ AFCIC/ITC with the position titles of designees. You must get HQ AFCIC/ITC approval before delegating this authority to a lower level. Send requests for waiver with justification to HQ AFCIC/ITC. Authorities are:

4.5.1. DCSs and chiefs of comparable offices or higher level at SAF or HQ USAF.

4.5.2. MAJCOM or FOA commanders.

4.5.3. HQ USAF/DPF, 1040 Air Force Pentagon, Washington DC 20330-1040 (for civilian personnel records).

4.5.4. Commander, Air Force Office of Special Investigations (AFOSI), Washington DC 20332-6001 (for AFOSI records).

5.5. Appeal Procedures. Individuals may request a denial review by writing to the Secretary of the Air Force, through the denial authority, within 60 calendar days after receiving a denial letter. The denial authority promptly sends a complete appeal package to HQ AFCIC/ITC. The package must include: (1) the original appeal letter; (2) the initial request; (3) the initial denial; (4) a copy of the record; (5) any

internal records or coordination actions relating to the denial; (6) the denial authority's comments on the appellant's arguments; and (7) the legal reviews.

5.5.2. HQ AFCIC/ITC reviews the denial and sends it to SAF/GCA through HQ USAF/JAG for legal review or staffing to grant or deny the appeal. SAF/GCA tells the requester the final Air Force decision and explains judicial review rights.

6.3. Submitting Notices for Publication in the *Federal Register*. At least 120 days before implementing a new system subject to this instruction, system managers must send a proposed notice, through the MAJCOM Privacy Office, to HQ AFCIC/ITC. Send notices electronically to afcicitcf@af.pentagon.mil using Microsoft Word. Mark changes to existing notices using the revision tool in Word. Follow format outlined in **Attachment 2**. On new systems, system managers must include a statement that a risk assessment was accomplished and is available should the OMB request it.

6.4. Reviewing Notices. System managers review their notices annually and submit changes to HQ AFCIC/ITC through the MAJCOM Privacy Office.

8.1. Requesting an Exemption. A system manager who believes that a system needs an exemption from some or all of the requirements of the PA should send a request to HQ AFCIC/ITC through the MAJCOM or FOA PA Officer. The request should detail the reasons for the exemption, the section of the Act that allows the exemption, and the specific subsections of the PA from which the system is to be exempted, with justification for each subsection.

8.3. Authorizing Exemptions. Only HQ AFCIC/ITC can approve exempt systems of records from any part of the Privacy Act. Denial authorities can withhold records using these exemptions *only* if HQ AFCIC/ITC previously approved and published an exemption for the system in the *Federal Register*. **Attachment 3** lists the systems of records that have approved exemptions.

9.1. Disclosure Considerations. Before releasing personal information to third parties, make sure it is authorized, consider the consequences, and check accuracy. You can release personal information to third parties when the subject agrees orally or in writing. Air Force members consent to releasing their home telephone number and address when they sign and check the "Do Consent" block on the AF Form 624, **Base/Unit Locator and PSC Directory** (see AFI 33-329, *Base and Unit Personnel Locators*).

9.1.2. You must get written consent before releasing any of these items of information. This list is not all inclusive:

9.1.2.1. Marital status.

9.1.2.2. Number and sex of dependents.

- 9.1.2.3. Civilian educational degrees and major areas of study (unless the request for the information relates to the professional qualifications for federal employment).
- 9.1.2.4. School and year of graduation.
- 9.1.2.5. Home of record.
- 9.1.2.6. Home address and phone.
- 9.1.2.7. Age and date of birth.
- 9.1.2.8. Present or future assignments for overseas or for routinely deployable or sensitive units.
- 9.1.2.9. Office and unit address and duty phone for overseas or for routinely deployable or sensitive units.
- 9.1.2.10. Race.
- 9.1.2.11. Educational level (unless the request for the information relates to the professional qualifications for federal employment).

9.7.3. Any activity that expects to participate in a matching program must contact HQ AFCIC/ITC immediately. System managers must prepare a notice for publication in the *Federal Register* with a Routine Use that allows disclosing the information for use in a matching program. Send the proposed system notice to HQ AFCIC/ITC. Allow 180 days for processing requests for a new matching program.

9.7.4. Record subjects must receive prior notice of a match. The best way to do this is to include notice in the Privacy Act Statement on forms used in applying for benefits. Coordinate computer matching statements on forms with HQ AFCIC/ITC through the MAJCOM PA Officer.

9.8. Privacy and the Web. Do not post personal information on publicly accessible DoD web sites unless clearly authorized by law and implementing regulation and policy. Additionally, do not post personal information on non-publicly accessible web sites unless it is mission essential and appropriate safeguards have been established. See AFIs 33-129 and 35-205.

10.2. Training Tools. Helpful aids include:

10.2.1. "The Privacy Act of 1974," a 32-minute film developed by the Defense Privacy Office. Consult your local audiovisual library.

10.2.2. A Manager's Overview, *What You Need to Know About the Privacy Act*. This Privacy overview is available on line at <http://www.afcic.hq.af.mil/Mission/access1.htm>.

NOTE: Formal school training groups that develop or modify blocks of instruction must send the material to HQ AFCIC/ITC for coordination.

11.1. Privacy Act Report (RCS: DD-DA&M[A]1379). By 1 March of each year, MAJCOM and FOA PA officers must send HQ AFCIC/ITC a report covering the previous calendar year. The report includes:

11.1.1. Total number of written requests for access that cite the PA or FOIA which are processed under this instruction.

- 11.1.2. Total number of requests wholly or partially granted.
- 11.1.3. Total number of requests denied and the PA exemptions used.
- 11.1.4. Total number of requests for which no record was found.
- 11.1.5. Total number of requests to amend records.
- 11.1.6. Total number of amendment requests wholly or partially granted.
- 11.1.7. Total number of amendment requests denied.
- 11.1.8. Specific recommendations for changes to the Act or the PA Program.

A2.1. System Identification Number. HQ AFCIC/ITC assigns the notice number, for example, F033 AF PC A, where "F" indicates "Air Force," the next number represents the series from AFMAN 37-139 (will convert to AFI 33-338) regarding records disposition, and the final letter group shows the system manager's command or DCS. The last character "A" indicates that this is the first notice for this series and system manager.

A2.13. Contesting Records Procedures. HQ AFCIC/ITC provides this standard caption.

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Title 5, United States Code, Section 552a, as amended, *The Privacy Act of 1974*
 Title 10, United States Code, Section 8013 *Secretary of the Air Force*
 Executive Order 9397, *Numbering System for Federal Accounts Relating to Individual Persons*
 32 Code of Federal Regulations 806b, *Air Force Privacy Act Program*
 DoD Directive 5400.11, *Department of Defense Privacy Program*, June 9, 1982
 DoD 5400.11-R, *Department of Defense Privacy Program*, August 1983
 AFI 33-202, *Computer Security*
 AFI 33-329, *Base and Unit Personnel Locators*
 AFRD 37-1, *Air Force Information Management*
 AFI 37-131, *Freedom of Information Act Program*
 AFMAN 37-139, *Records Disposition Schedule* (will convert to AFI 33-338)

Abbreviations and Acronyms

AETC Air Education and Training Command

AFA	Air Force Academy
AFBCMR	Air Force Board for Correction of Military Records
AFISA	Air Force Intelligence Services Agency
AFMC	Air Force Materiel Command
AFOSI	Air Force Office of Special Investigations
AFSC	Air Force Specialty Code
AFSCO	Air Force Security Clearance Office
AFSPA	Air Force Security Police Agency
ASCI	American Standard Code for Information Interchange
BAQ	Basic Allowance for Quarters
CFR	Code of Federal Regulations
DCS	Deputy Chief of Staff
DoD	Department of Defense
DR&MO	Defense Reutilization and Marketing Office
EAD	Entered on Active Duty
FOA	Field Operating Agency
FOIA	Freedom of Information Act
FOUO	For Official Use Only
IG	Inspector General
IMC	Interim Message Change
LE	Logistics and Engineering
MAJCOM	Major Command
MIRS	Management Information and Research System
MP	Military Personnel
MPC	Military Personnel Center
NARA	National Archives and Records Administration
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OPR	Office of Primary Responsibility
PA	Privacy Act
PAM	Privacy Act Monitor
PAS	Privacy Act Statement

RCS	Reports Control Symbol
SAF	Secretary of the Air Force
SAF/GCA	Deputy General Counsel for Fiscal, Ethics, and Civilian Personnel
SG	Surgeon General
SJA	Staff Judge Advocate
SP	Security Police
SSN	Social Security Number
US	United States
USAF	United States Air Force
U.S.C.	United States Code
VHA	Variable Housing Allowance

Terms

Access--Allowing individuals to review or receive copies of their records.

Amendment--The process of adding, deleting, or changing information in a system of records to make the data accurate, relevant, timely, or complete.

Computer Matching--A computerized comparison of two or more automated systems of records or a system of records with non-Federal records to establish or verify eligibility for payments under Federal benefit programs or to recover delinquent debts for these programs.

Confidential Source--A person or organization giving information under an express or implied promise of confidentiality made before September 27, 1975.

Confidentiality--An expressed and recorded promise to withhold the identity of a source or the information provided by a source. The Air Force promises confidentiality only when the information goes into a system with an approved exemption for protecting the identity of confidential sources.

Defense Data Integrity Board--Representatives from the Services and DoD who oversee, coordinate, and approve all DoD computer matching programs covered by the Act.

Denial Authority--The individuals with authority to deny requests for access or amendment of records under the Privacy Act.

Disclosure--Giving information from a system, by any means, to anyone other than the record subject.

Federal Benefit Program--A federally funded or administered program for individuals that provides cash or in-kind assistance (payments, grants, loans, or loan guarantees).

Individual--A living US citizen or a permanent resident alien.

Matching Agency--The agency that performs a computer match.

Minor--Anyone under the age of majority according to local state law. If there is no applicable state law, a minor is anyone under age 18. Military members and married persons are not minors, no matter what their chronological age.

Personal Identifier--A name, number, or symbol which is unique to an individual, usually the person's name or SSN.

Personal Information--Information about an individual other than items of public record.

Privacy Act Request--An oral or written request by an individual about his or her records in a system of records.

Recipient Agency--An agency or contractor that receives the records and actually performs the computer match.

Record--Any information about an individual.

Routine Use--A disclosure of records to individuals or agencies outside DoD for a use that is compatible with the purpose for which the Air Force created the records.

Source Agency--A federal, state, or local government agency that discloses records for the purpose of a computer match.

System Manager--The official who is responsible for managing a system of records, including policies and procedures to operate and safeguard it. Local system managers operate record systems or are responsible for part of a decentralized system.

System of Records--A group of records containing personal information retrieved by the subject's name, personal identifier, or individual identifier through a cross-reference system.

System Notice--The official public notice published in the *Federal Register* of the existence and content of the system of records.

Attachment 5

IC 2000-1 TO AFI 33-332, AIR FORCE PRIVACY ACT PROGRAM

8 NOVEMBER 2000

SUMMARY OF REVISIONS

This change incorporates interim change (IC) 2000-1 (**Attachment 5**). It changes training requirements to comply with SecDef (A&M) memo of 9 June 2000, and HQ AFCIC/ITC office symbol to HQ USAF/SCTIR.

This instruction implements AFPD 37-1, *Air Force Information Management* (will convert to AFPD 33-3). It also implements Department of Defense (DoD) Directive 5400.11, *Department of Defense Privacy Program*, June 9, 1982, and DoD 5400.11-R, *Department of Defense Privacy Program*, August 1983. It sets guidelines for collecting, safeguarding, maintaining, using, accessing, amending and disseminating personal data kept in systems of records to comply with the Air Force Privacy Act Program. It takes precedence over any other instruction that deals with personal privacy and rights of individuals regarding their records. This instruction applies to the Air Force Reserve, Air National Guard, and those combatant commands where the Air Force is the executive agent. Use of the term "MAJCOM" through this instruction includes MAJCOMs, FOAs, and DRUs. Send all supplements to this instruction to Headquarters United States Air Force (HQ USAF/SCTIR), 1250 Air Force Pentagon, Washington DC 20330-1250. Send recommended changes or comments to Headquarters Air Force Communications Agency (HQ AFCA/ITPP), 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, through appropriate channels, using AF Form 847, **Recommendation for Change of Publication**, with an information copy to HQ USAF/SCTIR. Refer to **Attachment 1** for a glossary of references and supporting information.

1.4.1. The Deputy Chief of Staff, Communications and Information (HQ USAF/SC), is the senior Air Force Privacy Official with overall responsibility for the Air Force Privacy Act Program.

1.4.3. The Director, Architecture and Interoperability (HQ USAF/SCT), manages the program through the Air Force Privacy Act Office in the Information Dissemination and Management Division (HQ USAF/SCTIR), who:

1.4.4. MAJCOM and FOA commanders, HQ USAF and Deputy Chiefs of Staff (DCS), and comparable officials, and SAF offices implement this instruction. Each HQ USAF and SAF office appoints a PA monitor. Send the name, office symbol, and phone number to HQ USAF/SCTIR.

1.4.5.3. Send the name, office symbol, and phone number to HQ USAF/SCTIR.

4.4.1.1. The system has an exemption approved by HQ USAF/SCTIR (as listed in **Attachment 3**, 32 CFR 806b.13, or published as a final rule in the *Federal Register*).

4.5. Denial Authorities. These officials or a designee may deny access or amendment of records as authorized by the Privacy Act. Send a letter to HQ USAF/SCTIR with the position titles of designees. You must get HQ USAF/SCTIR approval before delegating this authority to a lower level. Send requests for waiver with justification to HQ USAF/SCTIR. Authorities are:

5.5. Appeal Procedures. Individuals may request a denial review by writing to the Secretary of the Air Force, through the denial authority, within 60 calendar days after receiving a denial letter. The denial authority promptly sends a complete appeal package to HQ USAF/SCTIR. The package must include: (1) the original appeal letter; (2) the initial request; (3) the initial denial; (4) a copy of the record; (5) any internal records or coordination actions relating to the denial; (6) the denial authority's comments on the appellant's arguments; and (7) the legal reviews.

5.5.2. HQ USAF/SCTIR reviews the denial and sends it to SAF/GCA through HQ USAF/JAG for legal review or staffing to grant or deny the appeal. SAF/GCA tells the requester the final Air Force decision and explains judicial review rights.

6.3. Submitting Notices for Publication in the *Federal Register*. At least 120 days before implementing a new system subject to this instruction, system managers must send a proposed notice, through the MAJCOM Privacy Office, to HQ USAF/SCTIR. Send notices electronically to afscitif@af.pentagon.mil using Microsoft Word. Mark changes to existing notices using the revision tool in Word. Follow format outlined in **Attachment 2**. On new systems, system managers must include a statement that a risk assessment was accomplished and is available should the OMB request it.

6.4. Reviewing Notices. System managers review their notices annually and submit changes to HQ USAF/SCTIR through the MAJCOM Privacy Office.

8.1. Requesting an Exemption. A system manager who believes that a system needs an exemption from some or all of the requirements of the PA should send a request to HQ USAF/SCTIR through the MAJCOM or FOA PA Officer. The request should detail the reasons for the exemption, the section of the Act that allows the exemption, and the specific subsections of the PA from which the system is to be exempted, with justification for each subsection.

8.3. Authorizing Exemptions. Only HQ USAF/SCTIR can approve exempt systems of records from any part of the Privacy Act. Denial authorities can withhold records using these exemptions *only* if HQ USAF/SCTIR previously approved and published an exemption for the system in the *Federal Register*. **Attachment 3** lists the systems of records that have approved exemptions.

9.7.3. Any activity that expects to participate in a matching program must contact HQ USAF/SCTIR immediately. System managers must prepare a notice for publication in the *Federal Register* with a Rou-

Use that allows disclosing the information for use in a matching program. Send the proposed system notice to HQ USAF/SCTIR. Allow 180 days for processing requests for a new matching program.

9.7.4. Record subjects must receive prior notice of a match. The best way to do this is to include notice in the Privacy Act Statement on forms used in applying for benefits. Coordinate computer matching statements on forms with HQ USAF/SCTIR through the MAJCOM PA Officer.

10.1. Who Needs Training. The Privacy Act requires training for all persons involved in the design, development, operation and maintenance of any system of records. More specialized training is needed for personnel who may be expected to deal with the news media or the public, personnel specialists, finance officers, information managers, supervisors, and individuals working with medical and security records. Commanders will ensure that above personnel are trained annually in the principles and requirements of the Privacy Act.

10.2.2. A Manager's Overview, *What You Need to Know About the Privacy Act*. This overview is available on-line at <http://www.foia.af.mil>.

NOTE: Formal school training groups that develop or modify blocks of instruction must send the material to HQ USAF/SCTIR for coordination.

11.1. Privacy Act Report (RCS: DD-DA&M[A]1379). By 1 March of each year, MAJCOM and FOA PA officers must send HQ USAF/SCTIR a report covering the previous calendar year. The report includes:

11.2. Information Collections, Forms, and Records.

11.2.1. RCS: DD-DA&M[A]1379, Privacy Act Report, is mandated by this publication. See paragraph 11.1. for guidance.

11.2.2. The following forms are prescribed by this publication: AF Form 3227, Privacy Act Cover Sheet and AF Form 771, Accounting of Disclosures.

11.2.3. Retain and dispose of Privacy Act records according to AFI 37-139, *Records Disposition Schedule* (will convert to AFI 33-322, Vol. 4), Table 37-1, using the appropriate rule.

A2.1. System Identification Number. HQ USAF/SCTIR assigns the notice number, for example, F033 AF PC A, where "F" indicates "Air Force," the next number represents the series from AFMAN 37-139 (will convert to AFI 33-322, Vol. 4) regarding records disposition, and the final letter group shows the system manager's command or DCS. The last character "A" indicates that this is the first notice for this series and system manager.

A2.13. Contesting Records Procedures. HQ USAF/SCTIR provides this standard caption.