Dated: September 17, 2003.

Wayne A. Abernathy,

Assistant Secretary of the Treasury.

[FR Doc. 03–24226 Filed 9–24–03; 8:45 am]

BILLING CODE 4810–25–P

DEPARTMENT OF DEFENSE

Department of the Air Force

32 CFR Part 806b

[Air Force Instruction 33–332]

Privacy Act; Implementation

AGENCY: Department of the Air Force, DoD.

ACTION: Proposed rule.

SUMMARY: The Department of the Air Force proposes to revise the Privacy Act Program Instruction. The revision moves responsibility for the Air Force Privacy Program from AFCIC to AF–CIO; prescribes AFVA 33–276, Privacy Act Label as optional; adds the E-Gov Act of 2002 requirement for a Privacy Impact Assessment for all information systems that are new or have major changes; changes appeal processing from AFCIC to Air Force Legal Services Agency (AFLSA/JACL); adds Privacy Act warning language to use on information systems subject to the Privacy Act, includes guidance on sending personal information via e-mail; adds procedures on complaints; and provides guidance on recall rosters; social rosters; consent statements, systems of records operated by a contractor, and placing information on shared drives.

DATES: Submit comments on or before October 27, 2003.

ADDRESSES: Address all comments concerning this proposed rule to Mrs. Anne Rollins, Office of the Air Force Chief Information Officer, AF–CIO/P, 1155 Air Force Pentagon, Washington, DC 20330–1155.

FOR FURTHER INFORMATION CONTACT: Mrs. Anne Rollins, 703–601–4043.

SUPPLEMENTARY INFORMATION:

List of Subjects in 32 CFR Part 806b

Privacy.

For the reasons set forth in the preamble, the Department of the Air Force is revising 32 CFR part 806b as follows:

PART 806b—PRIVACY ACT PROGRAM

Subpart A—Overview of the Privacy Act Program

Sec.

Subpart B—Obtaining Law Enforcement Records and Confidentiality Promises

Subpart C—Collecting Personal Information

Subpart D—Giving Access to Privacy Act Records

Subpart E—Amending the Record

Subpart F—Appeals

Subpart G—Privacy Act Notifications

Subpart H—Privacy Impact Assessments

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

Subpart J—Protecting and Disposing of Records

Subpart K—Privacy Act Exemptions

Subpart L—Disclosing Records to Third Parties

Subpart M—Training

Authority: 5 U.S.C. 552a.

Subpart A—Overview of the Privacy Act Program

§ 806b.1 Summary of Revisions.

This part moves responsibility for the Air Force Privacy Program from AFCIC to AF–CIO; prescribes AFVA 33–276, Privacy Act Label as optional; adds the E-Gov Act of 2002 requirement for a Privacy Impact Assessment for all information systems that are new or have major changes; changes appeal processing from AFCIC to Air Force Legal Services Agency (AFLSA/JACL); adds Privacy Act warning language to use on information systems subject to the Privacy Act, includes guidance on sending personal information via e-mail; adds procedures on complaints; and provides guidance on recall rosters; social rosters; consent statements, systems of records operated by a contractor, and placing information on shared drives.

§ 806b.2 Basic Guidelines.

This part implements the Privacy Act of 1974 and applies to records on living U.S. citizens and permanent resident aliens that are retrieved by name or personal identifier. This part also provides guidance on collecting and disseminating personal information in general.

(a) Records that are retrieved by name or personal identifier are subject to Privacy Act (PA) requirements and are referred to as PA systems of records. The Air Force must publish notices in the **Federal Register**, describing the collection of information for new, changed or deleted systems to inform the public and give them an opportunity to comment before implementing or changing the system. (see Appendix D to this part).

(b) An official system of records is:

(1) Authorized by law or Executive Order.

(2) Needed to carry out an Air Force mission or function.

(3) Published in the **Federal Register**.

(c) The Air Force will not:

(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.

(2) Penalize or harass an individual for exercising rights guaranteed under the PA. We must reasonably help individuals exercise their rights under the PA.

(d) Air Force members will:

(1) Keep paper and electronic records that are retrieved by name or personal identifier only in approved PA systems published in the **Federal Register**.

(2) Collect, maintain, and use information in such systems, for purposes described in the published notice, to support programs authorized by law or Executive Order.

(3) Safeguard the records in the system and keep them the minimum time required.

(4) Ensure records are timely, accurate, complete, and relevant.

(5) Amend and correct records on request.

(6) Allow individuals to 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.

(7) Provide a review of decisions that deny individuals access to or amendment of their records through appellate procedures.

§ 806b.3 Violation Penalties.

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

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

(b) Disclosing information from a system of records to someone not entitled to the information.

(c) Obtaining someone else's records under false pretenses.

§ 806b.4 Privacy Act Complaints.

Process PA complaints or allegations of PA violations through the appropriate base or MAJCOM PA office, to the local systems manager. The base or MAJCOM PA officer directs the process and provides guidance to the system manager. The local systems manager will investigate complaints, or allegations of PA violations; will establish and review the facts when possible; interview individuals as needed; determine validity of the complaint; take appropriate corrective action; and ensure a response is sent to the complainant through the PA Officer. In cases where no system manager can be identified, the local PA officer will assume these duties. Issues that cannot be resolved at the local level will be elevated to the MAJCOM Privacy Office. When appropriate, local system managers will also: refer cases for more formal investigation, refer cases for command disciplinary action, and consult the servicing SJA. In unified combatant commands, process component unique system complaints through the respective component chain of command.

§ 806b.5 Personal Notes.

The Privacy Act does not apply to personal notes on individuals used as memory aids. Personal notes may become Privacy Act records if they are retrieved by name or other personal identifier and at least one of the following three conditions apply:

(a) Keeping or destroying the records is not at the sole discretion of the author;

(b) The notes are required by oral or written directive, regulation, or command policy; or

(c) They are shown to other agency personnel.

§ 806b.6 Systems of Records Operated by a Contractor.

Contractors who are required to operate or maintain a PA system of records by contract must follow this part for collecting, safeguarding, maintaining, using, accessing, amending and disseminating personal information. The record system affected is considered to be maintained by the Air Force and is subject to this part. Systems managers for offices who have contractors operating or maintaining such record systems must ensure the contract contains the proper PA clauses, and identify the record system number, as required by the Defense Acquisition Regulation and this part.

(a) Contracts for systems of records operated or maintained by a contractor will be reviewed annually by the appropriate MAJCOM Privacy Officer to ensure compliance with this part.

(b) Disclosure of personal records to a contractor for use in the performance of an Air Force contract is considered a disclosure within the agency under exception (b)(1) of the Privacy Act (see § 806b.47(a)).

§ 806b.7 Responsibilities.

(a) The Air Force Chief Information Officer (AF–CIO) is the senior Air Force Privacy Official with overall responsibility for the Air Force Privacy Act Program.

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

(c) The General Litigation Division, AFLSA/JACL, receives PA appeals and provides recommendations to the appellate authority. Service unique appeals, from unified combatant commands, should go through the respective chain of command.

(d) The Plans and Policy Directorate, Office of the Chief Information Officer (AF–CIO/P) manages the program through the Air Force PA Officer who:

(1) Administers procedures outlined in this part.

(2) Reviews publications and forms for compliance with this part.

(3) Reviews and approves proposed new, altered, and amended systems of records; and submits system notices and required reports to the Defense Privacy Office.

(4) Serves as the Air Force member on the Defense Privacy Board and the Defense Data Integrity Board.

(5) Provides guidance and assistance to MAJCOMs, FOAs, DRUs and combatant commands for which AF is executive agent in their implementation and execution of the Air Force Privacy Program. Insures availability of training and training tools for a variety of audiences.

(6) Provides advice and support to those commands to ensure that information requirements developed to collect or maintain personal data conform to PA standards; and that appropriate procedures and safeguards are developed, implemented, and maintained to protect the information.

(e) MAJCOM commanders, and Deputy Chiefs of Staff (DCS) and comparable officials at Secretary of the Air Force and Headquarters United States Air Force (HQ USAF) offices implement this part.

(f) 11th Communications Squadron (11 CS/SCS), will provide PA training and submit PA reports for HQ USAF and SAF offices.

(g) MAJCOM Commanders: Appoint a command PA officer, and send the name, office symbol, phone number, and e-mail address to AF–CIO/P.

(h) MAJCOM and HAF Functional CIOs:

(1) Review and provide final approval on Privacy Impact Assessments (PIA) (see Appendix F).

(2) Send a copy of approved PIAs to AF–CIO/P for forwarding to DoD and Office of Management and Budget (OMB).

(i) MAJCOM PA Officers:

(1) Train base PA officers. May authorize appointment of unit PA monitors to assist with implementation of the program.

(2) Promote PA awareness throughout the organization.

(3) Review publications and forms for compliance with this part (do forms require a Privacy Act Statement (PAS); is PAS correct?)

(4) Submit reports as required.

(5) Review system notices to validate currency.

(6) Evaluate the health of the program at regular intervals using this part as guidance.

(7) Review and provide recommendations on completed Privacy Impact Assessments (PIA) for information systems.

(8) Resolve complaints or allegations of PA violations.

(9) Review and process denial recommendations.

(10) Provide guidance as needed to functionals on implementing the Privacy Act.

(j) Base PA Officers:

(1) Provide guidance and training to base personnel.

(2) Submit reports as required.

(3) Review publications and forms for compliance with this part.

(4) Review system notices to validate currency.

(5) Direct investigations of complaints/violations.

(6) Evaluate the health of the program at regular intervals using this part as guidance.

(k) System Managers:

(1) Manage and safeguard the system.

(2) Train users on PA requirements.

(3) Protect records from unauthorized disclosure, alteration, or destruction.

(4) Prepare system notices and reports.

(5) Answer PA requests.

(6) Records of disclosures.

(7) Validate system notices annually.

(8) Investigate PA complaints.

(l) System owners and developers:

(1) Decide the need for, and content of systems.

(2) Evaluate PA requirements of information systems in early stages of development.

(3) Complete a PIA and submit to the PA Officer:

Subpart B—Obtaining Law Enforcement Records and Confidentiality Promises

§ 806b.8 Obtaining Law Enforcement Records.

The Commander, Air Force Office of Special Investigation (AFOSI); the Commander, Air Force Security Forces Center (HQ AFSFC); 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 U.S.C. 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.

§ 806b.9 Confidentiality Promises.

Promises of confidentiality must be prominently annotated in the record to protect from disclosure any ''confidential'' information under 5 United States Code 552a (k)(2), (k)(5), or (k)(7) of the Privacy Act.

Subpart C—Collecting Personal Information

§ 806b.10 How To Collect Personal Information.

Collect personal information directly from the subject of the record whenever possible. Only ask third parties when:

(a) You must verify information.

(b) You want opinions or evaluations.

(c) You can't contact the subject.

(d) You are doing so at the request of the subject individual.

§ 806b.11 When To Give Privacy Act Statements (PAS).

Give a PAS orally or in writing to the subject of the record when you are collecting information from them that will go in a system of records.

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.

(a) A PAS must include four items:

(1) *Authority:* The legal authority, that is, the U.S.C. or Executive Order authorizing the program the system supports.

(2) *Purpose:* The reason you are collecting the information and what you intend to do with it.

(3) *Routine Uses:* A list of where and why the information will be disclosed outside DoD.

(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.

(b) [Reserved].

§ 806b.12 Requesting the Social Security Number (SSN).

When asking an individual for his or her SSN, always give a Privacy Act Statement that tells the person: The legal authority for requesting it; the uses that will be made of the SSN; and whether providing the SSN is voluntary or mandatory. Do not deny anyone a legal right, benefit, or privilege for refusing to give their SSN 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.

(a) 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 to retrieve an existing record, you do not have to restate this information.

(b) Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons, 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.

(c) SSNs are personal and unique to each individual. Protect them as FOR OFFICIAL USE ONLY (FOUO). Within DoD, do not disclose them to anyone without an official need to know. Outside DoD, they are not releasable without the person's consent, or unless authorized under one of the 12 exceptions to the Privacy Act (*see* § 806b.47).

Subpart D—Giving Access to Privacy Act Records

§ 806b.13 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 may use a notary or 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).''

§ 806b.14 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 does not need to cite either Act if the records they want are contained in a system of records. Process the request under whichever Act gives the most information. When necessary, tell the requester which Act you used and why.

(a) 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*.

(b) Requesters should not use government equipment, supplies, stationery, postage, telephones, or official mail channels for making PA requests. System managers will process such requests and tell requesters that using government resources to make PA requests is not authorized.

(c) Tell the requester if a record exists and how to review the record. If possible, respond to requests within 10 workdays of receipt. 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.

(d) 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 Appendix E to this part; or it is published in this Section; or published as a final rule in the **Federal Register**. Give information in a form the requester can understand. If the system is exempt under the PA, provide any parts releasable under FOIA, with appeal rights (*see* Subpart F of this part), citing appropriate exemptions from the Privacy Act and FOIA, if applicable.

(e) 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.

§ 806b.15 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 fees for all pages for subsequent requests for the same records. Do not charge fees:

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

(b) For search.

(c) For reproducing a document for the convenience of the Air Force.

(d) For reproducing a record so the requester can review it.

§ 806b.16 Denying or Limiting Access.

System managers 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 (include the applicable exemption) to the denial authority through the legal office and the PA office. Judge Advocate (JA) offices will include a written legal opinion. The PA officer reviews the file, 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 (see Subpart F of this part). Before you deny a request for access to a record, make sure that:

(a) The system has an exemption approved by AF–CIO/P (as listed in Appendix E to this part, or published in this Section, or published as a final rule in the **Federal Register**).

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

(c) Nonexempt parts are segregated.

§ 806b.17 Special Provision for Certain Medical Records.

If a physician believes that disclosing requested medical records could harm the person's mental or physical health, you should:

(a) 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.

(b) Offer the services of a military physician other than one who provided treatment if naming the physician poses a hardship on the individual. The Privacy Act requires that we ultimately insure that the subject receives the records.

§ 806b.18 Third Party Information in a Privacy Act System of Record.

Ordinarily a person is entitled to their entire record under the Privacy Act. However, the law is not uniform regarding whether a subject is entitled to information that is not ''about'' him or her (for example, the home address of a third party contained in the subject's records). Consult your servicing SJA before disclosing third party information. Generally, if the requester will be denied a right, privilege or benefit, the requester must be given access to relevant portions of the file.

§ 806b.19 Information Compiled in Anticipation of Civil Action.

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.

§ 806b.20 Denial Authorities.

These officials or a designee may deny access or amendment of records as authorized by the Privacy Act. Send a letter to AF–CIO/P with the position titles of designees. Authorities are:

(a) DCSs and chiefs of comparable offices or higher level at SAF or HQ USAF or designees.

(b) MAJCOM, FOA, or DRU commanders or designees.

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

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

(e) Unified Commanders or designees.

Subpart E—Amending the Record

§ 806b.21 Amendment Reasons.

Individuals may ask to have their records amended to make them

accurate, timely, relevant, or complete. System managers will routinely correct a record if the requester can show that it is factually wrong (*e.g.*, date of birth is wrong).

§ 806b.22 Responding to Amendment Requests.

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

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

(c) 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.

§ 806b.23 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. Determinations not to amend such records constitutes a denial, and requesters may appeal (*see* Subpart F of this part).

(a) If the system manager decides not to amend the record, send a copy of the request, the record, and the recommended denial reasons to the denial authority through the legal office and the PA office. Legal offices will include a written legal opinion. The PA officer reviews the proposed denial and legal opinion and makes a recommendation to the denial authority.

(b) 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 (see Subpart F of this part).

§ 806b.24 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 part. Military personnel, other than USAF personnel, should pursue service-unique record corrections through their component chain of command.

§ 806b.25 Contents of PA Case Files.

Do not keep copies of disputed records in this file. File disputed records in their appropriate series. 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:

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

(b) Requests for access or amendment.

(c) Approvals, denials, appeals, and final review actions.

(d) Coordination actions and related papers.

Subpart F—Appeals

§ 806b.26 Appeal Procedures.

Individuals who receive a denial to their access or amendment request 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 AFLSA/JACL. The package must include: The original appeal letter; the initial request; the initial denial; a copy of the record; any internal records or coordination actions relating to the denial; the denial authority's comments on the appellant's arguments; and the legal reviews.

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

(b) AFLSA/JACL reviews the denial and provides a final recommendation to SAF/GCA. SAF/GCA tells the requester the final Air Force decision and explains judicial review rights.

(c) 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.

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

(e) The disputed part of the record must show that the requester filed a statement of disagreement.

(f) 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.

(g) 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.

Subpart G—Privacy Act Notifications

§ 806b.27 When To Include a Privacy Act Warning Statement in Publications.

Include a PA Warning Statement in each Air Force publication that requires collecting or keeping information in a system of records. Also include the Warning Statement when publications direct collection of the SSN, or any part of the SSN, from the individual. The warning statement will cite legal authority and when part of a record system, the PA 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.''

§ 806b.28 Warning Banners.

Information systems that contain information on individuals that is retrieved by name or personal identifier are subject to the Privacy Act. The Privacy Act requires these systems to have a PA system notice published in the **Federal Register** that covers the information collection before collection begins. In addition, all information systems subject to the Privacy Act will have warning banners displayed on the first screen (at a minimum) to assist in safeguarding the information. Use the following language for the banner: ''PRIVACY ACT INFORMATION—The information accessed through this system is FOR OFFICIAL USE ONLY and must be protected in accordance with the Privacy Act and AFI 33–332.''

§ 806b.29 Sending Personal Information Over Electronic Mail.

(a) Exercise caution before transmitting personal information over e-mail to ensure it is adequately safeguarded. Some information may be so sensitive and personal that e-mail may not be the proper way to transmit it. When sending personal information over e-mail within DoD, ensure: There is an official need; all addressee(s) (including ''cc'' addressees) are authorized to receive it under the Privacy Act; and it is protected from unauthorized disclosure, loss, or alteration. Protection methods may include encryption or password protecting the information in a separate Word document. When transmitting personal information over e-mail, add ''FOUO'' to the beginning of the subject line, followed by the subject, and apply the following statement at the *beginning* of the e-mail:

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

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

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

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

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

Subpart H—Privacy Impact Assessments

§ 806b.30 Evaluating Information Systems for Privacy Act Compliance.

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

(a) The PIA addresses what information is to be collected; why the information is being collected; the intended use of the information; with whom the information will be shared; what notice or opportunities for consent will be provided individuals regarding the information collected, and how that information is shared; secured; and whether a system of records is being created, or an existing system is being amended. The E-Government Act of 2002 requires PIAs to be conducted *before:*

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

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

(b) The system owner will conduct a PIA as outlined in Appendix F and send it to their MAJCOM Privacy Act office for review and final approval by the MAJCOM or HAF Functional CIO. The MAJCOM or HAF Functional CIO will send a copy of approved PIAs to AF-CIO/P, 1155 Air Force Pentagon, Washington DC 20330–1155; or e-mail *af.foia@pentagon.af.mil.*

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

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

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

§ 806b.31 Publishing System Notices.

The Air Force must publish notices in the **Federal Register** of new, changed, and deleted systems to inform the public of what records the Air Force keeps and give them an opportunity to comment before the system is implemented or changed. The PA also requires submission of new or significantly changed systems to the OMB and both houses of Congress before publication in the **Federal Register**. This includes:

(a) Starting a new system.

(b) Instituting significant changes to an existing system.

(c) Sending out data collection forms or instructions.

(d) Issuing a request for proposal or invitation for bid to support a new system.

§ 806b.32 Submitting Notices for Publication in the Federal Register.

At least 120 days before implementing a new system, or a major change to an existing system, subject to this part, system managers must send a proposed notice, through the MAJCOM Privacy Office, to AF–CIO/P. Send notices electronically to *af.foia@pentagon.af.mil* using Microsoft Word, using the Track Changes tool in Word to indicate additions/changes to existing notices. Follow the format outlined in Appendix D to this part. For new systems, system managers must include a statement that a risk assessment was accomplished and is available should the OMB request it.

§ 806b.33 Reviewing Notices.

System managers will review and validate their PA system notices annually and submit changes to AF–CIO/P through the MAJCOM Privacy Office.

Subpart J—Protecting and Disposing of Records

§ 806b.34 Protecting Records.

Maintaining information privacy is the responsibility of every federal employee, military member, and contractor who comes into contact with information in identifiable form. Protect information according to its sensitivity level. Consider the personal sensitivity of the information and the risk of disclosure, loss or alteration. Most information in systems of records is FOUO. Refer to DoD 5400.7–R/AF Supp, DoD Freedom of Information Act Program, for protection methods.

§ 806b.35 Balancing Protection.

Balance additional protection against sensitivity, risk and cost. In some situations, a password may be enough protection for an automated system with a log-on protocol. Others may require more sophisticated security protection based on the sensitivity of the information. Classified computer systems or those with established audit and password systems are obviously less vulnerable than unprotected files. Follow AFI 33–202, Computer Security, for procedures on safeguarding personal information in automated records.

(a) AF Form 3227, Privacy Act Cover Sheet, is optional and available for use with Privacy Act material. Use it to cover and protect personal information that you are using in office environments that are widely unprotected and accessible to many individuals. After use, such information should be protected as outlined in DoD 5400.7–R/AF Supp.

(b) Privacy Act Labels. Use of AFVA 33–276, Privacy Act Label, is optional to assist in protecting Privacy Act information on compact disks, diskettes, and tapes.

§ 806b.36 Disposing of Records.

You may use the following methods to dispose of records protected by the Privacy Act and authorized for destruction according to records retention schedules:

(a) Destroy by any method that prevents compromise, such as tearing, burning, or shredding, so long as the personal data is not recognizable and beyond reconstruction.

(b) Degauss or overwrite magnetic tapes or other magnetic medium.

(c) Dispose of paper products through the Defense Reutilization and Marketing Office or through activities that manage a base-wide recycling program. The

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.

Subpart K—Privacy Act Exemptions

§ 806b.37 Exemption Types.

There are two types of exemptions permitted by 5 U.S.C. 552a:

(a) A General exemption authorizes the exemption of a system of records from most parts of the PA.

(b) A Specific exemption authorizes the exemption of a system of records from only a few parts.

§ 806b.38 Authorizing Exemptions.

Only AF–CIO/P can approve exempt systems of records from any part of the Privacy Act. Denial authorities can withhold records using these exemptions only if AF–CIO/P previously approved and published an exemption for the system in the **Federal Register**. Appendix E to this part lists the systems of records that have approved exemptions with rationale.

§ 806b.39 Requesting an Exemption.

A system manager who believes that a system needs an exemption from some or all of the requirements of the PA will send a request to AF–CIO/P through the MAJCOM or FOA PA Officer. The request will 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.

§ 806b.40 Approved Exemptions.

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

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

(b) Classified information in any system of records (subsection (k)(1)).

(c) Law enforcement records (other than those covered by subsection (j)(2)). However, 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)).

(d) 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)).

(e) 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)).

(f) 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)).

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

Subpart L—Disclosing Records to Third Parties

§ 806b.41 Disclosure Considerations.

The Privacy Act requires the written consent of the subject before releasing personal information to third parties, unless one of the 12 exceptions of the Act apply (see § 806b.47). Use this checklist before releasing personal information to third parties: Make sure it is authorized under the Privacy Act; consider the consequences; and check the accuracy of the information. You can release personal information to third parties when the subject agrees 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).*

§ 806b.42 Social Rosters.

Before including personal information such as spouses names, home addresses, home phones, and similar information on social rosters or directories that are shared with groups of individuals, ask for signed consent statements. Otherwise, do not include the information. Consent statements must give the individual a choice to consent or not consent, and clearly tell the individual what information is being solicited, the purpose, to whom you plan to disclose the information, and that consent is voluntary. Maintain the signed statements until no longer needed.

§ 806b.43 Placing Personal Information on Shared Drives.

Personal information should never be placed on shared drives for access by groups of individuals unless each person has an official need to know the information to perform their job. Add appropriate access controls to ensure access by only authorized individuals. Recall rosters are FOUO because they contain personal information and should be shared with small groups at the lowest levels for official purposes to reduce the number of people with access to such personal information. Commanders and supervisors should give consideration to those individuals with unlisted phone numbers, who do not want their number included on the office recall roster. In those instances, disclosure to the Commander or immediate supervisor, or deputy, should normally be sufficient.

§ 806b.44 Personal Information That Requires Protection.

Following are some examples of information that is not releasable without the written consent of the subject. This list is not all inclusive.

(a) Marital status (single, divorced, widowed, separated).

(b) Number, name, and sex of dependents.

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

(d) School and year of graduation.

(e) Home of record.

(f) Home address and phone.

(g) Age and date of birth (year).

(h) Present or future assignments for overseas or for routinely deployable or sensitive units.

(i) Office and unit address and duty phone for overseas or for routinely deployable or sensitive units.

(j) Race/ethnic origin

(k) Educational level (unless the request for the information relates to the professional qualifications for Federal employment).

(l) Social Security Number.

§ 806b.45 Releasable Information.

Following are examples of information normally releasable to the public without the written consent of the subject. This list is not all inclusive.

(a) Name.

(b) Rank.

(c) Grade.

(d) Air Force specialty code.

(e) Pay (including base pay, special pay, all allowances except Basic Allowance for Quarters and Variable Housing Allowance).

(f) Gross salary for civilians.

(g) Past duty assignments, unless sensitive or classified.

(h) Present and future approved and announced stateside assignments.

(i) Position title.
(j) Office, unit address, and duty phone number (CONUS only).
(k) Date of rank.
(l) Entered on active duty date.
(m) Pay date.
(n) Source of commission.
(o) Professional military education.
(p) Promotion sequence number.
(q) Military awards and decorations.
(r) Duty status of active, retired, or reserve.
(s) Active duty official attendance at technical, scientific, or professional meetings.
(t) Biographies and photos of key personnel.
(u) Date of retirement, separation.

§ 806b.46 Disclosing Other Information.

Use these guidelines to decide whether to release information:
(a) Would the subject have a reasonable expectation of privacy in the information requested?
(b) 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.
(c) Balance the public interest against the individual's probable loss of privacy. Do not consider the requester's purpose, circumstances, or proposed use.

§ 806b.47 Rules for Releasing Privacy Act Information Without Consent of the Subject.

The Privacy Act prohibits disclosing personal information to anyone other than the subject of the record without their written consent. There are twelve exceptions to the ''no disclosure without consent'' rule. Those exceptions permit release of personal information without the individual's consent only in the following instances:
(a) Exception 1. DoD employees who have a need to know the information in the performance of their duties.
(b) Exception 2. In response to a FOIA request for information contained in a system of records about an individual and the FOIA requires release of the information.
(c) Exception 3. Agencies outside DoD only 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.
(d) Exception 4. The Bureau of the Census to plan or carry out a census or survey under Title 13, U.S.C. Section 8.
(e) Exception 5. 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.

(f) Exception 6. The Archivist of the United States and the National Archives and Records Administration to evaluate records for permanent retention. Records stored in Federal Records Centers remain under Air Force control.
(g) Exception 7. 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**.
(h) Exception 8. An individual or agency that needs the information for compelling health or safety reasons. The affected individual need not be the record subject.
(i) Exception 9. Either House of Congress, a congressional committee, or a subcommittee, for matters within their jurisdictions. The request must come from the committee chairman or ranking minority member (*see* AFI 90–401).
(j) Requests from a Congressional member acting on behalf of the record subject are evaluated under the routine use of the applicable system notice. If the material for release is sensitive, get a release statement.
(k) Requests from a Congressional member not on behalf of a committee or the record subject are properly analyzed under the FOIA, and not under the PA.
(l) Exception 10. The Comptroller General or an authorized representative of the General Accounting Office (GAO) to conduct official GAO business.
(m) Exception 11. A court of competent jurisdiction, with a court order signed by a judge.
(n) Exception 12. A consumer credit agency according to the Debt Collections Act when a published system notice lists this disclosure as a Routine Use.

§ 806b.48 Disclosing the Medical Records of Minors.

Air Force personnel may disclose the medical records of minors to their parents or legal guardians in conjunction with applicable Federal laws and guidelines. The laws of each state define the age of majority.
(a) 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.
(b) 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.

§ 806b.49 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. Retain disclosure accountings for 5 years after the disclosure, or for the life of the record, whichever is longer.
(a) 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:
(1) Release date.
(2) Description of information.
(3) Reason for release.
(4) Name and address of recipient.
(5) Some exempt systems let you withhold the accounting record from the subject.
(b) You may withhold information about disclosure accountings for law enforcement purposes at the law enforcement agency's request.

§ 806b.50 Computer Matching.

Computer matching programs electronically compare records from two or more automated systems that 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: Prepare a written agreement between participants; secure approval of the Defense Data Integrity Board; publish a matching notice in the **Federal Register** before matching begins; ensure full investigation and due process; and act on the information, as necessary.
(a) 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.

(b) 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.

(c) Any activity that expects to participate in a matching program must contact AF–CIO/P 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 AF–CIO/P. Allow 180 days for processing requests for a new matching program.

(d) 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 AF–CIO/P through the MAJCOM PA Officer.

§ 806b.51 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 .mil private Web sites unless authorized by the local commander, for official purposes, and an appropriate risk assessment is performed. *See* AFI 33–129, *Transmission of Information Via the Internet.*

(a) Ensure public Web sites comply with privacy policies regarding restrictions on persistent and third party cookies, and add appropriate privacy and security notices at major Web site entry points and Privacy Act statements or Privacy Advisories when collecting personal information. Notices must clearly explain where the collection or sharing of certain information may be optional, and notify users of how to provide consent.

(b) Include a Privacy Act Statement on the Web page if it collects information directly from an individual that we maintain and retrieve by his or her name or personal identifier (*i.e.*, SSN). We may only maintain such information in approved PA systems of records that are published in the **Federal Register**. Inform the visitor when the information is maintained and retrieved by name or personal identifier in a system of records; that the Privacy Act gives them certain rights with respect to the government's maintenance and use of information collected about them, and provide a link to the Air Force Privacy Act policy and system notices at *http://www.foia.af.mil.*

(c) Anytime a Web site solicits personally-identifying information, even when not maintained in a PA system of records, it requires a Privacy Advisory. The Privacy Advisory informs the individual why the information is solicited and how it will be used. Post the Privacy Advisory to the Web page where the information is being solicited, or through a well-marked hyperlink ''Privacy Advisory—Please refer to the Privacy and Security Notice that describes why this information is collected and how it will be used.''

Subpart M—Training

§ 806b.52 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.

§ 806b.53 Training Tools.

Helpful resources include:

(a) The Air Force FOIA Web page which includes a Privacy Overview, PA training slides, the Air Force systems of records notices, and links to the Defense Privacy Board Advisory Opinions, the DoD and Department of Justice Privacy Web pages. Go to *http://www.foia.af.mil.* Click on ''Resources.''

(b) ''The Privacy Act of 1974,'' a 32-minute film developed by the Defense Privacy Office. Contact the Joint Visual Information Activity at DSN 795–6543/7283 or commercial (717) 895–6543/7283, and ask for #504432 ''The Privacy Act of 1974.''

(c) A Manager's Overview, What You Need to Know About the Privacy Act. This overview gives you Privacy Act 101 and is available on-line at *http://www.foia.af.mil.*

(d) Training slides for use by the MAJCOM and base PA officers, available from the FOIA Web page at *http://www.foia.af.mil*, under ''Resources.''

Note: Formal school training groups that develop or modify blocks of instruction must send the material to AF–CIO/P for coordination.

§ 806b.54 Information Collections, Records, and Forms or Information Management Tools (IMT).

(a) Information Collections. No information collections are required by this publication.

(b) Records. Retain and dispose of PA records according to AFMAN 37–139, Records Disposition Schedule.

(c) Forms or IMTs (Adopted and Prescribed).

(1) Adopted Forms or IMTs. AF Form 624, Base/Unit Locator and PSC Directory, and AF Form 847, Recommendation for Change of Publication.

(2) Prescribed Forms or IMTs. AF Form 3227, Privacy Act Cover Sheet, AF Form 771, Accounting of Disclosures, and AF Visual Aid 33–276.

Appendix A to Part 806b—References

Title 5, U.S.C., Section 552a, as amended, The Privacy Act of 1974
Title 5, U.S.C., Section 552, The Freedom of Information Act
Title 10, U.S.C., Section 8013 Secretary of the Air Force
E.O. 9397, Numbering System for Federal Accounts Relating to Individual Persons
Pub. L. 100–235, The Computer Security Act of 1987
Pub. L. 100–503, The Computer Matching and Privacy Act of 1988
Pub. L. 104–13, Paperwork Reduction Act of 1995
Pub. L. 107–347, Section 208, E-Gov Act of 2002,
32 CFR part 806b, Air Force Privacy Act Program
Federal Register
DoD 6025.18R, DoD Health Information Privacy Regulation, 24 January 2003
DoDD 5400.11, DoD Privacy Program, December 13, 1999
DoD 5400.7–R/AF Supp, DoD Freedom of Information Act Program
DoD 5400.11–R, Department of Defense Privacy Program, August 1983
Defense Acquisition Regulation
OMB Circular A–130, Management of Federal Information Resources
AFPD 37–1, Air Force Information Management
AFI 33–129, Transmission of Information Via the Internet
AFI 33–202, Computer Security
AFI 33–329, Base and Unit Personnel Locators
AFI 33–360, Volume 2, Forms Management Program
AFI 90–401, Air Force Relations With Congress

AFMAN 37–139, Records Disposition Schedule
AFVA 33–276, Privacy Act Label

Appendix B to Part 806b—Abbreviations and Acronyms

AETC Air Education and Training Command
AF–CIO Air Force Chief Information Officer
AFBCMR Air Force Board for Correction of Military Records
AFLSA Air Force Legal Services Agency
AFMAN Air Force Manual
AFOSI Air Force Office of Special Investigations
AFPC Air Force Personnel Center
AFPD Air Force Policy Directive
CFR Code of Federal Regulations
DCS Deputy Chief of Staff
DoDD Department of Defense Directive
DRU Direct Reporting Unit
FOA Field Operating Agency
FOIA Freedom of Information Act
FOUO For Official Use Only
HAF Headquarters Air Force
HQ AFCA Headquarters Air Force Communications Agency
HQ AFSFC Headquarters Air Force Security Forces Center
HQ USAF Headquarters United States Air Force
IG Inspector General
IT Information Technology
MAJCOM Major Command
OMB Office of Management and Budget
OPR Office of Primary Responsibility
PA Privacy Act
PAS Privacy Act Statement
PIA Privacy Impact Assessment
Pub. L. Public Law
SAF Secretary of the Air Force
SFMIS Security Forces Management Information System
SG Surgeon General
SJA Staff Judge Advocate
SSN Social Security Number
US United States
USAFA Air Force Academy
U.S.C. United States Code

Appendix C to Part 806b—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.

Cookie. Data created by a Web server that is stored on a user's computer either temporarily for that session only or permanently on the hard disk (persistent cookie). It provides a way for the Web site to identify users and keep track of their preferences. It is commonly used to ''maintain the state'' of the session. A third-party cookie either originates on or is sent to a Web site different from the one you are currently viewing.

Defense Data Integrity Board. Composed of representatives from DoD components and the services 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 U.S. citizen or a permanent resident alien.

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 that 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.

Privacy Advisory. A statement required when soliciting personally-identifying information by an Air Force Web site and the information is not maintained in a system of records. The Privacy Advisory informs the individual why the information is being solicited and how it will be used.

Privacy Impact Assessment. A written assessment of an information system that addresses the information to be collected, the purpose and intended use; with whom the information will be shared; notice or opportunities for consent to individuals; how the information will be secured; and whether a new system of records is being created under the Privacy Act.

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.

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 retrieved by the individual'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.

Appendix D to Part 806b—Preparing A System Notice

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

System Identification Number. AF–CIO/P assigns the notice number, for example, F033 AF PC A, where ''F'' indicates ''Air Force,'' the next number represents the publication series number related to the subject matter, 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.

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

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.

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.

Categories of Records in the System. Describe in clear, plain language, 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.

Authority for Maintenance of the System. Cite the specific law or Executive Order that authorizes the program the records support. Cite the DoD directive/instruction or Air Force instruction(s) that authorizes the system of records. Always include titles with the citations.

Note: Executive Order 9397 authorizes using the SSN as a personal identifier. Include this authority whenever the SSN is used to retrieve records.

Purpose. Describe briefly and specifically what the Air Force does with the information collected.

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.

Polices and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage. State the medium in which the Air Force keeps the records; for example, in file folders, card files, microfiche, computer, or a combination of those methods. Storage does not refer to the storage container.

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

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.

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.

System Manager(s) and Address. List the position 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.

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.

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.

Contesting Records Procedures. AF–CIO/P provides this standard caption.

Record Source Categories. Show categories of individuals or other information sources for the system. Do not list confidential sources protected by 5 U.S.C., Section 552a (k)(2), (k)(5), or (k)(7).

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.

Appendix E to Part 806b—General And Specific Exemptions

(a) *General Exemption.* The following systems of records are exempt under 5 U.S.C., Section 552a(j)(2):

(1) *System identifier and name:* F071 AF OSI A, Counter Intelligence Operations and Collection Records.

(2) *System identifier and name:* F071 AF OSI C, Criminal Records.

(3) *System identifier and name:* F031 AF SP E, Security Forces Management Information System (SFMIS).

(i) *Exemption:* Parts of this system may be exempt pursuant to 5 U.S.C. 552a(j)(2) if information is compiled and maintained by a component of the agency which performs as its principle function any activity pertaining to the enforcement of criminal laws. Portions of this system of records may be exempt pursuant to 5 U.S.C. 552a(j)(2) from following subsections of 5 U.S.C. 552a(c)(c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), and (I), (e)(5), (e)(8), (f), and (g).

(ii) *Authority:* 5 U.S.C. 552a(j)(2).

(iii) *Reasons:* (A) To protect ongoing investigations and to protect from access criminal investigation information contained in this record system, so as not to jeopardize any subsequent judicial or administrative process taken as a result of information contained in the file.

(B) From subsection (c)(3) because the release of the disclosure accounting, for disclosures pursuant to the routine uses published for this system, would permit the subject criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(C) From subsection (c)(4) because an exemption is being claimed for subsection this subsection will not be applicable.

(D) From subsection (d) because access the records contained in this system would inform the subject of an investigation of existence of that investigation, provide subject of the investigation with information that might enable him to avoid detection, and would present a serious impediment to law enforcement.

(E) From subsection (e)(4)(H) because system of records is exempt from individual access pursuant to subsection (j) of the Privacy Act of 1974.

(F) From subsection (f) because this system of records has been exempted from access provisions of subsection (d).

(G) Consistent with the legislative purpose the Privacy Act of 1974, the Department of the Air Force will grant access to non-exempt material in the records being maintained. Disclosure will be governed by the Department of the Air Force's Privacy Instruction, but will be limited to the extent that identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered, the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of the above nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated above. The decisions to release information from these systems will be made on a case-by-case basis.

(4) *System identifier and name:* F071 AF OSI D, Investigative Support Records.

(5) *System identifier and name:* F031 AF SP A, Correction and Rehabilitation Records.

Exemption—Portions of this system that fall within 5 U.S.C. 552a(j)(2) are exempt from the following provisions of 5 U.S.C. 552a, Sections (c)(3) and (c)(4); (d)(1) through (d)(5); (e)(2) and (e)(3); (e)(4)(G) and (e)(4)(H), (e)(5); (f)(1) through (f)(5); (g)(1) through (g)(5); and (h) of the Act.

Authority—5 U.S.C. 552a(j)(2).

Reason—The general exemption will protect on going investigations and protect from access criminal investigation information contained in this record system so as not to jeopardize any subsequent judicial or administrative process taken as a result of information contained in the files.

(6) *System identifier and name:* F090 AF IG B, Inspector General Records.

(i) *Exemption:* (A) Parts of this system of records may be exempt pursuant to 5 U.S.C. 552a(j)(2) if the information is compiled and maintained by a component of the agency which performs as its principle function any activity pertaining to the enforcement of criminal laws. (B) Any portion of this system of records which falls within the provisions of 5 U.S.C. 552a(j)(2) may be exempt from the following subsections of 5 U.S.C. 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (H), and (I), (e)(5), (e)(8), (f), and (g).

(ii) *Authority:* 5 U.S.C. 552a(j)(2).

(iii) *Reasons:* (A) From subsection (c)(3) because the release of accounting of disclosure would inform a subject that he or she is under investigation. This information would provide considerable advantage to the subject in providing him or her with knowledge concerning the nature of the investigation and the coordinated investigative efforts and techniques employed by the cooperating agencies. This would greatly impede the Air Force IG's criminal law enforcement.

(B) From subsection (c)(4) and (d), because notification would alert a subject to the fact that an open investigation on that individual is taking place, and might weaken the on going investigation, reveal investigative techniques, and place confidential informants in jeopardy.

(C) From subsection (e)(1) because the nature of the criminal and/or civil investigative function creates unique problems in prescribing a specific parameter in a particular case with respect to what information is relevant or necessary. Also, information may be received which may relate to a case under the investigative jurisdiction of another agency. The maintenance of this information may be necessary to provide leads for appropriate law enforcement purposes and to establish patterns of activity that may relate to the jurisdiction of other cooperating agencies.

(D) From subsection (e)(2) because collecting information to the fullest extent possible directly from the subject individual may or may not be practical in a criminal and/or civil investigation.

(E) From subsection (e)(3) because supplying an individual with a form containing a Privacy Act Statement would tend to inhibit cooperation by many individuals involved in a criminal and/or civil investigation. The effect would be somewhat adverse to established investigative methods and techniques.

(F) From subsections (e)(4)(G), (H), and (I) because this system of records is exempt from the access provisions of subsection (d).

(G) From subsection (e)(5) because the requirement that records be maintained with attention to accuracy, relevance, timeliness, and completeness would unfairly hamper the investigative process. It is the nature of law enforcement for investigations to uncover the commission of illegal acts at diverse stages. It is frequently impossible to determine

initially what information is accurate, relevant, timely, and least of all complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light.

(H) From subsection (e)(8) because the notice requirements of this provision could present a serious impediment to law enforcement by revealing investigative techniques, procedures, and existence of confidential investigations.

(I) From subsection (f) because the agency's rules are inapplicable to those portions of the system that are exempt and would place the burden on the agency of either confirming or denying the existence of a record pertaining to a requesting individual might in itself provide an answer to that individual relating to an on going investigation. The conduct of a successful investigation leading to the indictment of a criminal offender precludes the applicability of established agency rules relating to verification of record, disclosure of the record to that individual, and record amendment procedures for this record system.

(J) From subsection (g) because this system of records should be exempt to the extent that the civil remedies relate to provisions of 5 U.S.C. 552a from which this rule exempts the system.

(iv) *Authority:* (A) Investigative material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identity of a confidential source.

Note: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(B) Therefore, portions of this system of records may be exempt pursuant to 5 U.S.C. 552a(k)(2) from the following subsections of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H) and (I), and (f).

(v) *Reasons:* (A) From subsection (c)(3) because to grant access to the accounting for each disclosure as required by the Privacy Act, including the date, nature, and purpose of each disclosure and the identity of the recipient, could alert the subject to the existence of the investigation. This could seriously compromise case preparation by prematurely revealing its existence and nature; compromise or interfere with witnesses or make witnesses reluctant to cooperate; and lead to suppression, alteration, or destruction of evidence.

(B) From subsections (d) and (f) because providing access to investigative records and the right to contest the contents of those records and force changes to be made to the information contained therein would seriously interfere with and thwart the orderly and unbiased conduct of the investigation and impede case preparation. Providing access rights normally afforded under the Privacy Act would provide the subject with valuable information that would allow interference with or compromise of witnesses or render witnesses reluctant to cooperate; lead to suppression, alteration, or destruction of evidence; enable individuals to conceal their wrongdoing or mislead the course of the investigation; and result in the secreting of or other disposition of assets that would make them difficult or impossible to reach in order to satisfy any Government claim growing out of the investigation or proceeding.

(C) From subsection (e)(1) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(D) From subsections (e)(4)(G) and (H) because this system of records is compiled for investigative purposes and is exempt from the access provisions of subsections (d) and (f).

(E) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses, and informants.

(F) Consistent with the legislative purpose of the Privacy Act of 1974, the AF will grant access to nonexempt material in the records being maintained. Disclosure will be governed by AF's Privacy Instruction, but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal or civil violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered, the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of the above nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated above. The decisions to release information from these systems will be made on a case-by-case basis.

(b) *Specific Exemptions.* The following systems of records are subject to the specific exemptions shown:

(1) *Classified records.*

(i) All records in any systems of records that are properly classified according to current Executive Order are exempt from 5 U.S.C. 552a(c)(3); (d); (e)(4)(G), (H), (I); and (f), regardless of whether the entire system is otherwise exempt or not.

(ii) *Authority.* 5 U.S.C. 552a(k)(1).

(2) *System identifier and name:* F036 USAFA K, Admissions Records.

(i) *Exemption.* Parts of this system of records (Liaison Officer Evaluation and Selection Panel Candidate Evaluation) are exempt from 5 U.S.C. 552a(d), (e)(4)(H), and (f), but only to the extent that disclosure would reveal the identity of a confidential source.

(ii) *Authority.* 5 U.S.C. 552a(k)(7).

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

(3) *System identifier and name:* F036 AFPC N, Air Force Personnel Test 851, Test Answer Sheets.

(i) *Exemption.* This system is exempt from 5 U.S.C. 552a(c)(3); (d); (e)(4) (G), (H), and (I); and (f).

(ii) *Authority.* 5 U.S.C. 552a(k)(6).

(iii) *Reasons.* To protect the objectivity of the promotion testing system by keeping the test questions and answers in confidence.

(4) *System identifier and name:* F036 USAFA A, Cadet Personnel Management System.

(i) *Exemption.* Parts of this system are exempt from 5 U.S.C. 552a(d), (e)(4)(H), and (f), but only insofar as disclosure would reveal the identity of a confidential source.

(ii) *Authority.* 5 U.S.C. 552a(k)(7).

(iii) *Reasons.* To maintain the candor and integrity of comments needed to evaluate an Air Force Academy cadet for commissioning in the Air Force.

(5) *System identifier and name:* F036 AETC I, Cadet Records.

(i) *Exemption.* Portions of this system (Detachment Professional Officer Course Selection Rating Sheets; Air Force Reserve Officer Training Corps (AFROTC) Form 0–24–Disenrollment Review; Memoranda for Record and Staff Papers with Staff Advice, Opinions, or Suggestions) are exempt from 5 U.S.C. 552a(c)(3); (d); (e)(4)(G) and (H), and (f), but only to the extent that disclosure would reveal the identity of a confidential source.

(ii) *Authority.* 5 U.S.C. 552a(k)(5).

(iii) *Reasons.* To protect the identity of a confidential source who furnishes information necessary to make determinations about the qualifications, eligibility, and suitability of cadets for graduation and commissioning in the Air Force.

(6) *System identifier and name:* F044 AF SG Q, Family Advocacy Program Records.

(i) *Exemption:*

(A) Investigative material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identify of a confidential source.

Note: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(B) Investigative material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information

may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(C) Therefore, portions of the system of records may be exempt pursuant to 5 U.S.C. 552a(c)(3) and (d), but only to the extent that disclosure would reveal the identity of a confidential source.

(ii) *Authority:* 5 U.S.C. 552a(k)(2) and (k)(5).

(iii) *Reasons:* From subsections (c)(3) and (d) because the exemption is needed to encourage those who know of exceptional medical or educational conditions or family maltreatments to come forward by protecting their identities and to protect such sources from embarrassment or recriminations, as well as to protect their right to privacy. It is essential that the identities of all individuals who furnish information under an express promise of confidentiality be protected. Granting individuals access to information relating to criminal and civil law enforcement, as well as the release of certain disclosure accounting, could interfere with ongoing investigations and the orderly administration of justice, in that it could result in the concealment, alteration, destruction, or fabrication of information; could hamper the identification of offenders or alleged offenders and the disposition of charges; and could jeopardize the safety and well being of parents and their children. Exempted portions of this system also contain information considered relevant and necessary to make a determination as to qualifications, eligibility, or suitability for Federal employment and Federal contracts, and that was obtained by providing an express or implied promise to the source that his or her identity would not be revealed to the subject of the record.

(7) *System identifier and name:* F036 AF PC A, Effectiveness/Performance Reporting System.

(i) *Exemptions*—Brigadier General Selectee Effectiveness Reports and Colonel and Lieutenant Colonel Promotion Recommendations with close out dates on or before January 31,1991, may be exempt from subsections of 5 U.S.C. 552a(c)(3); (d); (e)(4)(H); and (f).

(ii) *Authority*—5 U.S.C. 552a(k)(7).

(iii) *Reasons*—Subsection (c)(3) because making the disclosure accounting available to the individual may compromise express promises of confidentiality by revealing details about the report and identify other record sources, which may result in circumvention of the access exemption. Subsection (d) because individual disclosure compromises express promises of confidentiality conferred to protect the integrity of the promotion rating system. Subsection (e)(4)(H) because of and to the extent that portions of this record system are exempt from the individual access provisions of subsection (d). Subsection (f) because of and to the extent that portions of this record system are exempt from the individual access provisions of subsection (d).

(8) [Reserved.]

(9) *System identifier and name:* F036 AFDP A, Files on General Officers and Colonels Assigned to General Officer Positions.

(i) *Exemption.* This system is exempt from 5 U.S.C. 552a(c)(3); (d); (e)(4)(G), (H), and (I); and (f), but only to the extent that disclosure would reveal the identity of a confidential source.

(ii) *Authority.* 5 U.S.C. 552a(k)(7).

(iii) *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.

(10) *System identification and name:* F036 AF PC O, General Officer Personnel Data System.

(i) *Exemption*—Air Force General Officer Promotion and Effectiveness Reports with close out dates on or before January 31, 1991, may be exempt from subsections of 5 U.S.C. 552a(c)(3); (d); (e)(4)(H); and (f).

(ii) *Authority*—5 U.S.C. 552a(k)(7).

(iii) *Reason*—Subsection (c)(3) because making the disclosure accounting available to the individual may compromise express promises of confidentiality by revealing details about the report and identify other record sources, which may result in circumvention of the access exemption. Subsection (d) because individual disclosure compromises express promises of confidentiality conferred to protect the integrity of the promotion rating system. Subsection (e)(4)(H) because of and to the extent that portions of this record system are exempt from the individual access provisions of subsection (d). Subsection (f) because of and to the extent that portions of this record system are exempt from the individual access provisions of subsection (d).

(11) *System identifier and name:* F036 AFPC K, Historical Airman Promotion Master Test File.

(i) *Exemption.* This system is exempt from 5 U.S.C. 552a(c)(3); (d); (e)(4) (G), (H), and (I); and (f).

(ii) *Authority.* 5 U.S.C. 552a(k)(6).

(iii) *Reasons.* To protect the integrity, objectivity, and equity of the promotion testing system by keeping test questions and answers in confidence.

(12) [Reserved].

(13) *System identifier and name:* F071 AF OSI F, Investigative Applicant Processing Records.

(i) *Exemption.* This system is exempt from 5 U.S.C. 552a(c)(3); (d); (e)(4) (G), (H), and (I); and (f), but only to the extent that disclosure would reveal the identity of a confidential source.

(ii) *Authority.* 5 U.S.C. 552a(k)(5).

(iii) *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.

(14) *System identifier and name:* F036 USAFA B, Master Cadet Personnel Record (Active/Historical).

(i) *Exemptions.* Parts of these systems are exempt from 5 U.S.C. 552a(d), (e)(4)(H), and (f), but only to the extent that they would reveal the identity of a confidential source.

(ii) *Authority.* 5 U.S.C. 552a(k)(7).

(iii) *Reasons.* To maintain the candor and integrity of comments needed to evaluate a cadet for commissioning in the Air Force.

(15) *System identifier and name:* F031 497IG A, Sensitive Compartmented Information Personnel Records.

(i) *Exemption.* This system is exempt from 5 U.S.C. 552a(a)(3); (d); (e)(4) (G), (H), and (I); and (f), but only to the extent that disclosure would reveal the identity of a confidential source.

(ii) *Authority.* 5 U.S.C. 552a(k)(2) and (k)(5).

(iii) *Reasons.* To protect the identity of sources to whom proper promises of confidentiality have been made during investigations. Without these promises, sources will often be unwilling to provide information essential in adjudicating access in a fair and impartial manner.

(16) *System identifier and name:* F071 AF OSI B, Security and Related Investigative Records.

(i) *Exemption.* This system is exempt from 5 U.S.C. 552a(c)(3); (d); (e)(4) (G), (H), and (I); and (f), but only to the extent that disclosure would reveal the identity of a confidential source.

(ii) *Authority.* 5 U.S.C. 552a(k)(5).

(iii) *Reasons.* To protect the identity of those who give information in confidence for personnel security and related investigations. Fear of harassment could cause sources to refuse to give this information in the frank and open way needed to pinpoint those areas in an investigation that should be expanded to resolve charges of questionable conduct.

(17) *System identifier and name:* F031 497IG B, Special Security Case Files.

(i) *Exemption.* This system is exempt from 5 U.S.C. 552a(c)(3); (d), (e)(4) (G), (H), and (I); and (f), but only to the extent that disclosure would reveal the identity of a confidential source.

(ii) *Authority.* 5 U.S.C. 552a(k)(5).

(iii) *Reasons.* To protect the identity of those who give information in confidence for personnel security and related investigations. Fear of harassment could cause sources to refuse to give this information in the frank and open way needed to pinpoint those areas in an investigation that should be expanded to resolve charges of questionable conduct.

(18) *System identifier and name:* F031 AF SP N, Special Security Files.

(i) *Exemption.* This system is exempt from 5 U.S.C. 552a(c)(3); (d); (e)(4) (G), (H), and (I); and (f), but only to the extent that disclosure would reveal the identity of a confidential source.

(ii) *Authority.* 5 U.S.C. 552a(k)(5).

(iii) *Reasons.* To protect the identity of those who give information in confidence for personnel security and related investigations. Fear of harassment could cause them to refuse to give this information in the frank and open way needed to pinpoint areas in an investigation that should be expanded to resolve charges of questionable conduct.

(19) *System identifier and name:* F036 AF PC P, Applications for Appointment and Extended Active Duty Files.

(i) *Exemption.* Parts of this system of records are exempt from 5 U.S.C. 552a(d), but only to the extent that disclosure would reveal the identity of a confidential source.

(ii) *Authority.* 5 U.S.C. 552a(k)(5).

(iii) *Reasons.* To protect the identity of confidential sources who furnish information necessary to make determinations about the qualifications, eligibility, and suitability of health care professionals who apply for Reserve of the Air Force appointment or interservice transfer to the Air Force.

(20) *System identifier and name:* F051 AF JA F, Courts-Martial and Article 15 Records.

(i) *Exemption.* Portions of this system of records may be exempt pursuant to 5 U.S.C. 552a(j)(2) from the following subsection of 5 U.S.C. 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (H) and (I), (e)(5), (e)(8), (f), and (g).

(ii) *Exemption.* Portions of this system of records may be exempt pursuant to 5 U.S.C. 552a(k)(2) from the following subsection of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H) and (I), and (f).

(iii) *Authority:* 5 U.S.C. 552a(j)(2) and (k)(2).

(iv) *Reason:*

(1) From subsection (c)(3) because the release of the disclosure accounting, for disclosures pursuant to the routine uses published for this system, would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(2) From subsection (c)(4) because an exemption is being claimed for subsection (d), this subsection will not be applicable.

(3) From subsection (d) because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(4) From subsection (e)(1) because in the course of criminal investigations information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(5) From subsection (e)(2) because in a criminal investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection.

(6) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life and physical safety of confidential informants.

(7) From subsections (e)(4)(G) and (H) because this system of records is exempt from individual access pursuant to subsections (j) and (k) of the Privacy Act of 1974.

(8) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(9) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of intelligence necessary for effective law enforcement.

(10) From subsection (e)(8) because the individual notice requirements of subsection(e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue search authorizations and could reveal investigative techniques and procedures.

(11) From subsection (f) because this system of records has been exempted from the access provisions of subsection (d).

(12) From subsection (g) because this system of records is compiled for law enforcement purposes and has been exempted from the access provisions of subsections (d) and(f).

(13) Consistent with the legislative purpose of the Privacy Act of 1974, the Department of the Air Force will grant access to nonexempt material in the records being maintained. Disclosure will be governed by the Department of the Air Force's Privacy Instruction, but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered, the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of the above nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated above. The decisions to release information from these systems will be made on a case-by-case basis.

(21) *System identifier and name:* F036 AF DPG, Military Equal Opportunity and Treatment.

(i) *Exemption:* Investigatory material compiled for law enforcement purposes may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information except to the extent that disclosure would reveal the identity of a confidential source. Portions of this system of records may be exempt pursuant to 5 U.S.C.552a(d), (e)(4)(H), and (f).

(ii) *Authority:* 5 U.S.C. 552a(k)(2).

(iii) *Reasons:*

(1) From subsection (d) because access to the records contained in this system would inform the subject of an investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection, and would present a serious impediment to law enforcement. In addition, granting individuals access to information collected while an Equal Opportunity and Treatment clarification/investigation is in progress conflicts with the just, thorough, and timely completion of the complaint, and could possibly enable individuals to interfere, obstruct, or mislead those clarifying/investigating the complaint.

(2) From subsection (e)(4)(H) because this system of records is exempt from individual access pursuant to subsection (k) of the Privacy Act of 1974.

(3) From subsection (f) because this system of records has been exempted from the access provisions of subsection (d).

(4) Consistent with the legislative purpose of the Privacy Act of 1974, the Department of the Air Force will grant access to nonexempt material in the records being maintained. Disclosure will be governed by the Department of the Air Force's Privacy Instruction, but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered, the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of the above nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated above. The decisions to release information from this system will be made on a case-by-case basis.

(22) *System identifier and name:* F051 AF JA I, Commander Directed Inquiries.

(i) *Exemption:*

(1) Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information except to the extent that disclosure would reveal the identity of a confidential source.

Note: When claimed, this exemption allows limited protection of investigative

reports maintained in a system of records used in personnel or administrative actions.

(2) Any portion of this system of records which falls within the provisions of 5 U.S.C. 552a(k)(2) may be exempt from the following subsections of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f).

(ii) *Authority:* 5 U.S.C. 552a(k)(2).

(iii) *Reasons:* (A) From subsection (c)(3) because to grant access to the accounting for each disclosure as required by the Privacy Act, including the date, nature, and purpose of each disclosure and the identity of the recipient, could alert the subject to the existence of the investigation. This could seriously compromise case preparation by prematurely revealing its existence and nature; compromise or interfere with witnesses or make witnesses reluctant to cooperate; and lead to suppression, alteration, or destruction of evidence.

(B) From subsections (d) and (f) because providing access to investigative records and the right to contest the contents of those records and force changes to be made to the information contained therein would seriously interfere with and thwart the orderly and unbiased conduct of the investigation and impede case preparation. Providing access rights normally afforded under the Privacy Act would provide the subject with valuable information that would allow interference with or compromise of witnesses or render witnesses reluctant to cooperate; lead to suppression, alteration, or destruction of evidence; enable individuals to conceal their wrongdoing or mislead the course of the investigation; and result in the secreting of or other disposition of assets that would make them difficult or impossible to reach in order to satisfy any Government claim growing out of the investigation or proceeding.

(C) From subsection (e)(1) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(D) From subsections (e)(4)(G) and (H) because this system of records is compiled for investigative purposes and is exempt from the access provisions of subsections (d) and (f).

(E) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants.

(F) Consistent with the legislative purpose of the Privacy Act of 1974, the Air Force will grant access to nonexempt material in the records being maintained. Disclosure will be governed by Air Force's Privacy Regulation, but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal or civil violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered, the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of the above nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated above. The decisions to release information from these systems will be made on a case-by-case basis.

(23) *System identifier and name:* F031 DoD A, Joint Personnel Adjudication System.

(i) *Exemption:*

(1) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(2) Therefore, portions of this system may be exempt pursuant to 5 U.S.C. 552a(k)(5) from the following subsections of 5 U.S.C. 552a(c)(3), (d), and (e)(1).

(ii) *Authority:* 5 U.S.C. 552a(k)(5).

(iii) *Reasons:*

(A) From subsection (c)(3) and (d) when access to accounting disclosures and access to or amendment of records would cause the identity of a confidential source to be revealed. Disclosure of the source's identity not only will result in the Department breaching the promise of confidentiality made to the source but it will impair the Department's future ability to compile investigatory material for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access to classified information. Unless sources can be assured that a promise of confidentiality will be honored, they will be less likely to provide information considered essential to the Department in making the required determinations.

(B) From (e)(1) because in the collection of information for investigatory purposes, it is not always possible to determine the relevance and necessity of particular information in the early stages of the investigation. In some cases, it is only after the information is evaluated in light of other information that its relevance and necessity becomes clear. Such information permits more informed decision-making by the Department when making required suitability, eligibility, and qualification determinations.

(24) *System identifier and name:* F033 AF A, Information Requests-Freedom of Information Act.

(i) *Exemption:* During the processing of a Freedom of Information Act request, exempt materials from 'other' systems of records may in turn become part of the case record in this system. To the extent that copies of exempt records from those other systems of records are entered into this system, the Department of the Air Force hereby claims the same exemptions for the records from those 'other' systems that are entered into this system, as claimed for the original primary system of which they are a part.

(ii) *Authority:* 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), (k)(3), (k)(4), (k)(5), (k)(6), and (k)(7).

(iii) *Reasons:* Records are only exempt from pertinent provisions of 5 U.S.C. 552a to the extent such provisions have been identified and an exemption claimed for the original record, and the purposes underlying the exemption for the original record still pertain to the record which is now contained in this system of records. In general, the exemptions were claimed in order to protect properly classified information relating to national defense and foreign policy, to avoid interference during the conduct of criminal, civil, or administrative actions or investigations, to ensure protective services provided the President and others are not compromised, to protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations, and to preserve the confidentiality and integrity of Federal evaluation materials. The exemption rule for the original records will identify the specific reasons why the records are exempt from specific provisions of 5 U.S.C. 552a.

(25) *System identifier and name:* F033 AF B, Privacy Act Request Files.

(i) *Exemption:* During the processing of a Privacy Act request, exempt materials from other systems of records may in turn become part of the case record in this system. To the extent that copies of exempt records from those 'other' systems of records are entered into this system, the Department of the Air Force hereby claims the same exemptions for the records from those 'other' systems that are entered into this system, as claimed for the original primary system of which they are a part.

(ii) *Authority:* 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), (k)(3), (k)(4), (k)(5), (k)(6), and (k)(7).

(iii) *Reason:* Records are only exempt from pertinent provisions of 5 U.S.C. 552a to the extent such provisions have been identified and an exemption claimed for the original record, and the purposes underlying the exemption for the original record still pertain to the record which is now contained in this system of records. In general, the exemptions were claimed in order to protect properly classified information relating to national defense and foreign policy, to avoid interference during the conduct of criminal, civil, or administrative actions or investigations, to ensure protective services provided the President and others are not compromised, to protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations, and to preserve the confidentiality and integrity of Federal evaluation materials. The exemption rule for the original records will identify the specific reasons why the records are exempt from specific provisions of 5 U.S.C. 552a.

Appendix F to Part 8066—Privacy Impact Assessment

Section A—Introduction and Overview

The Privacy Act Assessment. The Air Force recognizes the importance of protecting the privacy of individuals, to ensure sufficient protections for the privacy of personal information as we implement citizen-centered e-Government. Privacy issues must

be addressed when systems are being developed, and privacy protections must be integrated into the development life cycle of these automated systems. The vehicle for addressing privacy issues in a system under development is the Privacy Impact Assessment (PIA). The PIA process also provides a means to assure compliance with applicable laws and regulations governing individual privacy.

(a) Purpose. The purpose of this document is to:

(1) Establish the requirements for addressing privacy during the systems development process.

(2) Describe the steps required to complete a PIA.

(3) Define the privacy issues you will address in the PIA.

(b) Background. The Air Force is responsible for ensuring the privacy, confidentiality, integrity, and availability of personal information. The Air Force recognizes that privacy protection is both a personal and fundamental right. Among the most basic of individuals' rights is an expectation that the Air Force will protect the confidentiality of personal, financial, and employment information. Individuals also have the right to expect that the Air Force will collect, maintain, use, and disseminate identifiable personal information and data only as authorized by law and as necessary to carry out agency responsibilities. Personal information is protected by the following:

(1) Title 5, U.S.C. 552a, The Privacy Act of 1974, as amended, which affords individuals the right to privacy in records maintained and used by Federal agencies.

Note: 5 U.S.C. 552a includes Public Law (Pub. L.) 100–503, The Computer Matching and Privacy Act of 1988.

(2) Pub. L. 100–235, The Computer Security Act of 1987, which establishes minimum security practices for Federal computer systems.

(3) OMB Circular A–130, Management of Federal Information Resources, which provides instructions to Federal agencies on how to comply with the fair information practices and security requirements for operating automated information systems.

(4) Pub. L. 107–347, Section 208, E-Gov Act of 2002, which aims to ensure privacy in the conduct of federal information activities.

(5) Title 5, U.S.C. 552, The Freedom of Information Act, as amended, which provides for the disclosure of information maintained by Federal agencies to the public while allowing limited protections for privacy.

(6) DoDD 5400.11, Department of Defense Privacy Program, December 13, 1999.

(7) DoD 5400.11–R, Department of Defense Privacy Program, August 1983.

(8) AFI 33–332, Air Force Privacy Act Program.

(c) The Air Force Privacy Office is in the Office of the Air Force Chief Information Officer (AF–CIO), Directorate of Plans and Policy, and is responsible for overseeing Air Force implementation of the Privacy Act.

Section B—Privacy and Systems Development

System Privacy. Rapid advancements in computer technology make it possible to store and retrieve vast amounts of data of all kinds quickly and efficiently. These advancements have raised concerns about the impact of large computerized information systems on the privacy of data subjects. Public concerns about highly integrated information systems operated by the government make it imperative to commit to a positive and aggressive approach to protecting individual privacy. AF–CIO is requiring the use of this PIA in order to ensure that the systems the Air Force develops protect individuals' privacy. The PIA incorporates privacy into the development life cycle so that all system development initiatives can appropriately consider privacy issues from the earliest stages of design.

(a) What is a Privacy Impact Assessment? The PIA is a process used to evaluate privacy in information systems. The process is designed to guide system owners and developers in assessing privacy through the early stages of development. The process consists of privacy training, gathering data from a project on privacy issues, and identifying and resolving the privacy risks. The PIA process is described in detail in Section C, Completing a Privacy Impact Assessment.

(b) When is a PIA Done? The PIA is initiated in the early stages of the development of a system and completed as part of the required system life cycle reviews. Privacy must be considered when requirements are being analyzed and decisions are being made about data usage and system design. This applies to all of the development methodologies and system life cycles used in the Air Force.

(c) Who completes the PIA? Both the system owner and system developers must work together to complete the PIA. System owners must address what data is to be used, how the data is to be used, and who will use the data. The system developers must address whether the implementation of the owner's requirements presents any threats to privacy.

(d) What systems have to complete a PIA? Accomplish PIAs when:

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

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

(3) Systems as described above that are undergoing major modifications.

(e) The Air Force or MAJCOM Privacy Act Officer reserves the right to request that a PIA be completed on any system that may have privacy risks.

Section C—Completing a Privacy Impact Assessment

The PIA. This section describes the steps required to complete a PIA. These steps are summarized in Table A4.1, Outline of Steps for Completing a PIA.

Training. Training on the PIA will be available, on request, from the MAJCOM Privacy Act Officer. The training consists of describing the PIA process and provides detail about the privacy issues and privacy questions to be answered to complete the PIA. MAJCOM Privacy Act Officers may use Appendix F, Sections A, B, D, and E for this purpose. The intended audience is the personnel responsible for writing the PIA document.

The PIA Document. Preparing the PIA document requires the system owner and developer to answer the privacy questions in Section E. A brief explanation should be written for each question. Issues that do not apply to a system should be noted as ''Not Applicable.'' During the development of the PIA document, the MAJCOM Privacy Act Officer will be available to answer questions related to the PIA process and other concerns that may arise with respect to privacy.

Review of the PIA Document. Submit the completed PIA document to the MAJCOM Privacy Act Office for review. The purpose of the review is to identify privacy risks in the system.

Approval of the PIA. The system life cycle review process (Command, Control, Communications, Computers, and Intelligence Support Plan) will be used to validate the incorporation of the design requirements to resolve the privacy risks. MAJCOM and HAF Functional CIOs will issue final approval of the PIA.

TABLE A4.1.—OUTLINE OF STEPS FOR COMPLETING A PIA

Step	Who	Procedure
1	System Owner, and Developer	Request and complete Privacy Impact Assessment (PIA) Training.
2	System Owner, and Developer	Answer the questions in Section E, Privacy Questions. For assistance contact your MAJCOM Privacy Act Officer.
3	System Owner, and Developer	Submit the PIA document to the MAJCOM Privacy Act Officer.

TABLE A4.1.—OUTLINE OF STEPS FOR COMPLETING A PIA—Continued

Step	Who	Procedure
4	MAJCOM Privacy Act Officer	Review the PIA document to identify privacy risks from the information provided. The MAJCOM Privacy Act Officer will get clarification from the owner and developer as needed.
5	System Owner and Developer, MAJCOM Privacy Act Officer.	The System Owner, Developer and the MAJCOM Privacy Act Officer should reach agreement on design requirements to resolve all identified risks.
6	System Owner, Developer, and MAJCOM Privacy Act Officer.	Participate in the required system life cycle reviews to ensure satisfactory resolution of identified privacy risks to obtain formal approval from the MAJCOM or HAF Functional CIO.
7	MAJCOM or HAF Functional CIO	Issue final approval of PIA, and send a copy to AF–CIO/P for forwarding to DoD and OMB.
8	AF–CIO/P	When feasible, publish PIA on FOIA Web page (*http://www.foia.af.mil*)

Section D—Privacy Issues in Information Systems

Privacy Act of 1974, 5 U.S.C. 552a as Amended

Title 5, U.S.C., 552a, The Privacy Act of 1974, as amended, requires Federal Agencies to protect personally identifiable information. It states specifically: Each agency that maintains a system of records shall:

Maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President;

Collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs;

Maintain all records used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;

Establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

Definitions

Accuracy—within sufficient tolerance for error to assure the quality of the record in terms of its use in making a determination.

Completeness—all elements necessary for making a determination are present before such determination is made.

Determination—any decision affecting an individual which, in whole or in part, is based on information contained in the record and which is made by any person or agency.

Necessary—a threshold of need for an element of information greater than mere relevance and utility.

Record—any item, collection or grouping of information about an individual and identifiable to that individual that is maintained by an agency.

Relevance—limitation to only those elements of information that clearly bear on the determination(s) for which the records are intended.

Routine Use—with respect to the disclosure of a record, the use of such record outside DoD for a purpose that is compatible with the purpose for which it was collected.

System of Records—a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

Timeliness—sufficiently current to ensure that any determination based on the record will be accurate and fair.

Information and Privacy

To fulfill the commitment of the Air Force to protect personal information, several issues must be addressed with respect to privacy.

The use of information must be controlled.

Information may be used only for a necessary and lawful purpose.

Individuals must be informed in writing of the principal purpose and routine uses of the information being collected from them.

Information collected for a particular purpose should not be used for another purpose without the data subject's consent unless such other uses are specifically authorized or mandated by law.

Any information used must be sufficiently accurate, relevant, timely and complete to assure fair treatment of the individual.

Given the availability of vast amounts of stored information and the expanded capabilities of information systems to process the information, it is foreseeable that there will be increased requests to share that information. With the potential expanded uses of data in automated systems it is important to remember that information can only be used for the purpose for which it was collected unless other uses are specifically authorized or mandated by law. If the data is to be used for other purposes, then the public must be provided notice of those other uses.

These procedures do not in themselves create any legal rights, but are intended to express the full and sincere commitment of the Air Force to protect individual privacy rights and which provide redress for violations of those rights.

Data in the System

The sources of the information in the system are an important privacy consideration if the data is gathered from other than Air Force records. Information collected from non-Air Force sources should be verified, to the extent practicable, for accuracy, that the information is current, and complete. This is especially important if the information will be used to make determinations about individuals.

Access to the Data

Who has access to the data in a system must be defined and documented. Users of the data can be individuals, other systems, and other agencies. Individuals who have access to the data can be system users, system administrators, system owners, managers, and developers. When individuals are granted access to a system, their access should be limited, where possible, to only that data needed to perform their assigned duties. If individuals are granted access to all of the data in a system, procedures need to be in place to deter and detect browsing and unauthorized access. Other systems are any programs or projects that interface with the system and have access to the data. Other agencies can be International, Federal, state, or local entities that have access to Air Force data.

Attributes of the Data

When requirements for the data to be used in the system are being determined, those requirements must include the privacy attributes of the data. The privacy attributes are derived from the legal requirements imposed by *The Privacy Act of 1974.* First, the data must be *relevant* and *necessary* to accomplish the purpose of the system. Second, the data must be *complete, accurate,* and *timely.* It is important to ensure the data has these privacy attributes in order to assure fairness to the individual in making decisions based on the data.

Maintenance of Administrative Controls

Automation of systems can lead to the consolidation of processes, data, and the controls in place to protect the data. When administrative controls are consolidated, they should be evaluated so that all necessary controls remain in place to the degree necessary to continue to control access to and use of the data.

Document record retention procedures and coordinate them with the MAJCOM Command Records Manager.

Section E—Privacy Questions

Data in the System

1. Generally describe the information to be used in the system.

2. What are the sources of the information in the system?

a. What Air Force files and databases are used?

b. What Federal Agencies are providing data for use in the system?

c. What State and local agencies are providing data for use in the system?

d. What other third party sources will data be collected from?

e. What information will be collected from the employee?

3. Is data accurate and complete?

a. How will data collected from sources other than Air Force records and the subject be verified for accuracy?

b. How will data be checked for completeness?

c. Is the data current? How do you know?

4. Are the data elements described in detail and documented? If yes, what is the name of the document?

Access to the Data

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?

2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

3. Will users have access to all data on the system or will the user's access be restricted? Explain.

4. What controls are in place to prevent the misuse (*e.g.*, browsing) of data by those having access?

5. Does the system share data with another system?

a. Do other systems share data or have access to data in this system? If yes, explain.

b. Who will be responsible for protecting the privacy rights of the employees affected by the interface?

6. Will other agencies have access to the data in the system?

a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?

b. How will the data be used by the agency?

c. Who is responsible for assuring proper use of the data?

d. How will the system ensure that agencies only get the information they are entitled to under applicable laws?

Attributes of the Data

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

2. Will the system create new data about an individual?

a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

b. Will the new data be placed in the individual's record?

c. Can the system make determinations about the record subject that would not be possible without the new data?

d. How will the new data be verified for relevance and accuracy?

3. Is data being consolidated?

a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

4. How will the data be retrieved? Is it retrieved by personal identifier? If yes, explain.

Maintenance of Administrative Controls

(1) a. Explain how the system and its use will ensure equitable treatment of record subjects.

b. If the system is operated at more than one location, how will consistent use of the system and data be maintained?

c. Explain any possibility of disparate treatment of individuals or groups.

(2) a. Coordinate proposed maintenance and disposition of the records with the MAJCOM Command Records Manager.

b. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

(3) a. Is the system using technologies in ways that the Air Force has not previously employed?

b. How does the use of this technology affect personal privacy?

(4) a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.

c. What controls will be used to prevent unauthorized monitoring?

(5) a. Under which Systems of Record notice does the system operate? Provide number and name.

b. If the system is being modified, will the system of record require amendment or revision? Explain.

Pamela D. Fitzgerald,

Air Force Federal Register Liaison Officer.

[FR Doc. 03–24058 Filed 9–24–03; 8:45 am]

BILLING CODE 5001–5–P

ADVISORY COUNCIL ON HISTORIC PRESERVATION

36 CFR Part 800

RIN 3014–AA27

Protection of Historic Properties

AGENCY: Advisory Council on Historic Preservation.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Advisory Council on Historic Preservation (ACHP) is submitting proposed amendments to the regulations setting forth how Federal agencies take into account the effects of their undertakings on historic properties and afford the ACHP a reasonable opportunity to comment, pursuant to section 106 of the National Historic Preservation Act. Most of the proposed amendments respond to recent court decisions which held that the ACHP could not force a Federal agency to change its determinations regarding whether its undertakings affected or adversely affected historic properties, and that section 106 does not apply to undertakings that are merely subject to State or local regulation administered pursuant to a delegation or approval by a Federal agency. Another proposed amendment clarifies the time period for objections to ''No Adverse Effect'' findings. The last proposed amendments clarify that the ACHP can propose an exemption to the section 106 process on its own initiative, rather than needing a Federal agency to make such a proposal.

DATES: Submit comments on or before October 27, 2003.

ADDRESSES: Address all comments concerning this proposed rule to the Executive Director, Advisory Council on Historic Preservation, 1100 Pennsylvania Avenue, NW., Suite 809, Washington, DC 20004. Fax (202) 606–8672. You may submit electronic comments to: *achp@achp.gov.* For electronic comments, please type ''Regs Amendment 2003'' in the subject line of the e-mail.

FOR FURTHER INFORMATION CONTACT: Javier Marqués, Advisory Council on Historic Preservation, 1100 Pennsylvania Avenue, NW., Suite 809, Washington, DC 20004 (202) 606–8503.

SUPPLEMENTARY INFORMATION:

I. Background

Section 106 of the National Historic Preservation Act of 1966, as amended, 16 U.S.C. 470f, requires Federal agencies to take into account the effects of their undertakings on properties included, or eligible for inclusion, in the