

(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).