

## SUBCHAPTER A—ADMINISTRATION

### PARTS 800–805 [RESERVED]

### PART 806—AIR FORCE FREEDOM OF INFORMATION ACT PROGRAM

- Sec.
- 806.1 Summary of revisions.
  - 806.2 Applicability.
  - 806.3 Public information.
  - 806.4 Definitions.
  - 806.5 Responsibilities.
  - 806.6 Prompt action on requests.
  - 806.7 Use of exemptions.
  - 806.8 Description of requested record.
  - 806.9 Referrals.
  - 806.10 Records management.
  - 806.11 FOIA reading rooms.
  - 806.12 Record availability.
  - 806.13 5 U.S.C. 552 (a)(2) materials.
  - 806.14 Other materials.
  - 806.15 FOIA exemptions.
  - 806.16 For official use only.
  - 806.17 Release and processing procedures.
  - 806.18 Initial determinations.
  - 806.19 Reasonably segregable portions.
  - 806.20 Records of non-U.S. government source.
  - 806.21 Appeals.
  - 806.22 Time limits.
  - 806.23 Delay in responding to an appeal.
  - 806.24 Fee restrictions.
  - 806.25 Annual report.
  - 806.26 Addressing FOIA requests.
  - 806.27 Samples of Air Force FOIA processing documents.
  - 806.28 Records with special disclosure procedures.
  - 806.29 Administrative processing of Air Force FOIA requests.
  - 806.30 FOIA exempt information examples.
  - 806.31 Requirements of 5 U.S.C. 552(b)(4) to submitters of nongovernment contract-related information.

APPENDIX A TO PART 806—REFERENCES  
APPENDIX B TO PART 806—ABBREVIATIONS AND ACRONYMS  
APPENDIX C TO PART 806—TERMS

AUTHORITY: 5 U.S.C. 552.

SOURCE: 64 FR 72808, Dec. 28, 1999, unless otherwise noted.

#### § 806.1 Summary of revisions.

This part makes this guidance an Air Force supplement to the DoD regulation at 32 CFR part 286. It transfers responsibility for the Air Force Freedom of Information Act (FOIA) Program from the Office of the Secretary of the Air Force (SAF/AAI) to Headquarters

United States Air Force (HQ USAF/SC) and Headquarters Air Force Communications and Information Center/Corporate Information Division (HQ AFCIC/ITC); contains significant changes and additions to implement the Electronic Freedom of Information Act (EFOIA) Amendments of 1996; addresses electronic records; increases time limits to 20 working days; adds procedures for multiple tracking and expedited processing of requests; changes annual report date and content; adds major command (MAJCOM) inspectors general (IG), MAJCOM Directors of Inquiries (IGQ), and wing commanders as initial denial authorities (IDAs).

#### § 806.2 Applicability.

A list of Air Force MAJCOMs, field operating agencies (FOAs), and Direct Reporting Units (DRUs) is at § 806.26.

#### § 806.3 Public information.

(a) *Functional requests.* Air Force elements may receive requests for government information or records from the public that do not refer to the FOIA. Often these requests are sent to a public affairs office (PAO) or a specific unit. All releases of information from Air Force records, whether the requester cites the FOIA or not, must comply with the principles of the FOIA and this part. If the requested material contains personal privacy information that the Air Force must withhold, it is particularly important to handle that “functional” request as a request under the FOIA and coordinate it with the appropriate FOIA office and an Air Force attorney. Regardless of the nature of the functional request, if the responding element denies the release of information from Air Force records, then control the request as a FOIA and follow FOIA denial procedures for records withheld (cite the pertinent FOIA exemption and give the requester FOIA appeal rights).

(b) HQ AFCIC/ITC will make the Air Force handbook and guide for requesting records available on the World Wide Web (WWW) from Air ForceLINK, at <http://www.foia.af.mil/handbook.htm>.

**§ 806.4 Definitions.**

(a) *Electronic reading room (ERR)*. Rooms established on Internet web sites for public access to FOIA-processed (a)(2)(D) records.

(b) *FOIA request*. This includes FOIA requests made by members of Congress either on their own behalf or on behalf of one of their constituents. Process FOIA requests from members of Congress in accordance with this Air Force supplement. Air Force-affiliated requesters, to include military and civilian employees, should not use government equipment, supplies, stationery, postage, telephones, or official mail channels to make FOIA requests.

(1) Simple requests can be processed quickly with limited impact on the responding units. The request clearly identifies the records with no (or few) complicating factors involved. There are few or no responsive records. Only one installation is involved and there are no outside Office of Primary Responsibility (OPRs). There are no classified or nongovernment records. No deliberative process/privileged materials are involved. The responsive records contain no (or limited) personal privacy information and do not come from a Privacy Act system of records. No time extensions are anticipated.

(2) Complex requests take substantial time and cause significant impact on responding units. Complications and delays are likely. Records sought are massive in volume. Multiple organizations must review/coordinate on requested records. Records are classified; originated with a nongovernment source; are part of the Air Force's decision-making process; or are privileged.

(c) *Government Information Locator Service (GILS)*. GILS is an automated on-line card catalog of publicly accessible information. The Office of Management and Budget (OMB) Bulletin 95-01, December 7, 1994, and OMB Memorandum, February 6, 1998, mandates that all federal agencies create a GILS record for information available to the public. The DoD GILS resides on DefenseLINK, the official DoD home page, at <http://www.defenselink.mil/locator/index.html>.

(d) *Initial denial authority*. Only approved IDAs may deny all or parts of

records. FOIA managers may: initially deny fee category claims, requests for expedited processing, and waiver or reduction of fees; review fee estimates; and sign "no records" responses. IDAs are the deputy chiefs of staff and chiefs of comparable offices or higher at HQ USAF and Secretary of the Air Force (SAF), and MAJCOM commanders, Deputy Chiefs of Staff and chiefs of comparable offices or higher at HQ USAF and SAF may name one additional position as denial authority. MAJCOM commanders may appoint two additional positions at the headquarters and also the wing commander at base level. MAJCOM IGs and MAJCOM Directors of Inquiries (IGQ) may act as IDAs for IG records. MAJCOM FOIA managers must notify HQ AFCIC/ITC in writing (by facsimile, e-mail, or regular mail) of IDA position titles. Send position titles only—no names. HQ AFCIC/ITC sends SAF/IGQ a copy of the correspondence designating IDA positions for IG records. When the commander changes the IDA designee position, MAJCOM FOIA managers will advise HQ AFCIC/ITC immediately. In the absence of the designated IDA, the individual filling/assuming that position acts as an IDA, however; all denial documentation must reflect the position title of the approved or designated IDA, even if in an acting capacity (for example, Acting Director of Communications and Information, Headquarters Air Combat Command).

(e) *Office of primary responsibility (OPR)*. A DoD element that either prepared, or is responsible for, records identified as responsive to a FOIA request. OPRs coordinate with the office of corollary responsibility (OCR) and FOIA managers to assist IDAs in making decisions on FOIA requests.

(f) *OCR*. A DoD element with an official interest in, and/or collateral responsibility for, the contents of records identified as responsive to a FOIA request, even though those records were either prepared by, or are the primary responsibility of, a different DoD element. OCRs coordinate with OPRs and FOIA managers to assist IDAs in making decisions on FOIA requests.

(g) *Appellate authority.* The SAF has designated the Deputy General Counsel, Fiscal, Ethics, and Civilian Personnel (SAF/GCA) as the FOIA appellate authority.

(h) *Reading room.* Any place where a member of the public may view FOIA records.

#### § 806.5 Responsibilities.

(a) The Director, Communications and Information (HQ USAF/SC) has overall responsibility for the Air Force FOIA Program. The Corporate Information Division (HQ AFCIC/ITC) administers the procedures necessary to implement the Air Force FOIA Program, submits reports to the Director, Freedom of Information and Security Review (DFOISR), and provides guidance and instructions to MAJCOMs. Responsibilities of other Air Force elements follow.

(b) SAF/GCA makes final decisions on FOIA administrative appeals.

(c) Installation commanders will: Comply with FOIA electronic reading room (ERR) requirements by establishing a FOIA site on their installation public web page and making frequently requested records (FOIA-processed (a)(2)(D)) records available through links from that site, with a link to the Air Force FOIA web page at <http://www.foia.af.mil>. See § 806.12(c).

(d) MAJCOM commanders implement this instruction and appoint a FOIA manager, in writing. Send the name, phone number, office symbol, and e-mail address to HQ AFCIC/ITC, 1250 Air Force Pentagon, Washington, DC 20330-1250.

(e) Air Force attorneys review FOIA responses for legal sufficiency, provide legal advice to OPRs, disclosure authorities, IDAs, and FOIA managers, and provide written legal opinions when responsive records (or portions of responsive records) are withheld. Air Force attorneys ensure factual and legal issues raised by appellants are considered by IDAs prior to sending the FOIA appeal files to the Secretary of the Air Force's designee for final action.

(f) Disclosure authorities and IDAs apply the policies and guidance in this instruction, along with the written recommendations provided by staff ele-

ments, when considering what decisions to make on pending FOIA actions. Where any responsive records are denied, the IDA tells the requesters the nature of records or information denied, the FOIA exemption supporting the denial, the reasons the records were not released, and gives the requester the appeal procedures. In addition, on partial releases, IDAs must ensure requesters can see the placement and general length of redactions with the applicable exemption indicated. This procedure applies to all media, including electronic records. Providing placement and general length of redacted information is not required if doing so would harm an interest protected by a FOIA exemption. When working FOIA appeal actions for the appellate authority review:

(1) IDAs grant or recommend continued denial (in full or in part) of the requester's appeal of the earlier withholding of responsive records, or adverse determination (for example, IDAs may release some or all of the previously denied documents).

(2) IDAs reassess a request for expedited processing due to demonstrated compelling need, overturning or confirming the initial determination made by the FOIA manager.

(3) When an IDA denies any appellate action sought by a FOIA requester, the IDA, or MAJCOM FOIA manager (for no record, fee, fee estimates, or fee category appeals) will indicate in writing that the issues raised in the FOIA appeal were considered and rejected (in full or in part). Include this written statement in the file you send to the Secretary of the Air Force in the course of a FOIA appeal action. Send all appeal actions through the MAJCOM FOIA office.

(g) OPRs:

(1) Coordinate the release or denial of records requested under the FOIA with OPRs, FOIA offices, and with Air Force attorneys on proposed denials.

(2) Provide requested records. Indicate withheld parts of records annotated with FOIA exemption. Ensure requesters can see the placement and general length of redactions. This procedure applies to all media, including

## § 806.6

## 32 CFR Ch. VII (7-1-12 Edition)

electronic records. Providing placement and general length of redacted information is not required if doing so would harm an interest protected by a FOIA exemption.

(3) Provide written recommendations to the disclosure authority to determine whether or not to release records, and act as declassification authority when appropriate.

(4) Make frequently requested records (FOIA-processed (a)(2)(D)) available to the public in the FOIA ERR via the Internet. As required by AFIs 33-129, Transmission of Information Via the Internet, and 35-205, Air Force Security and Policy Review Program, OPRs request clearance of these records with the PAO before posting on the WWW, and coordinate with JA and FOIA office prior to posting. The FOIA manager, in coordination with the functional OPR or the owner of the records, will determine qualifying records, after coordination with any interested OCRs.

(5) Complete the required GILS core record for each FOIA-processed (a)(2)(D) record.

(6) Manage ERR records posted to the installation public web page by updating or removing them when no longer needed. Software for tracking number of hits may assist in this effort.

(h) FOIA managers:

(1) Ensure administrative correctness of all FOIA actions processed.

(2) Control and process FOIA requests.

(3) Obtain recommendations from the OPR for records.

(4) Prepare or coordinate on all proposed replies to the requester. FOIA managers may sign replies to requesters when disclosure authorities approve the total release of records. If the MAJCOM part directs the OPR to prepare the reply, the OPR will coordinate their reply with the FOIA office.

(5) Make determinations as to whether or not the nature of requests are simple or complex where multitrack FOIA request processing queues exist.

(6) Approve or initially deny any requests for expedited processing.

(7) Provide interim responses to requesters, as required.

(8) Provide a reading room for inspecting and copying records.

(9) Provide training.

(10) Review publications for compliance with this part.

(11) Conduct periodic program reviews.

(12) Approve or deny initial fee waiver requests.

(13) Make the initial decision on chargeable fees.

(14) Collect fees.

(15) Send extension notices.

(16) Submit reports.

(17) Sign "no record" responses.

(18) Provide the requester the basis for any adverse determination (i.e., no records, fee denials, fee category determinations, etc.) in enough detail to permit the requester to make a decision whether or not to appeal the actions taken, and provide the requester with appeal procedures.

(i) On appeals, FOIA managers:

(1) Reassess a fee category claim by a requester, overturning or confirming the initial determination.

(2) Reassess a request for expedited processing due to demonstrated compelling need, overturning or confirming the initial determination.

(3) Reassess a request for a waiver or reduction of fees, overturning or confirming the initial determination.

(4) Review a fee estimate, overturning or confirming the initial determination.

(5) Confirm that no records were located in response to a request.

(j) The base FOIA manager acts as the FOIA focal point for the FOIA site on the installation web page.

(k) When any appellate action sought by a FOIA requester is denied by an IDA or FOIA manager for authorized actions, the IDA or FOIA manager will indicate, in writing, that the issues raised in the FOIA appeal were considered and rejected (in full or in part). Include this written statement in the file you send to the Secretary of the Air Force in the course of a FOIA appeal action. Send all appeal actions through the MAJCOM FOIA office.

### § 806.6 Prompt action on requests.

(a) Examples of letters to FOIA requesters (e.g., response determinations and interim responses) are included in § 806.27.

(b) Multitrack processing. (1) Examples of letters to FOIA requesters (e.g.,

## Department of the Air Force, DoD

## § 806.10

letters to individuals who have had their FOIA request placed in the complex track) are included in §806.27.

(2) Simple requests can be processed quickly, with limited impact on the responding units. The request clearly identifies the records with no (or few) complicating factors involved. There are few or no responsive records, only one installation is involved, there are no outside OPRs, no classified or non-government records, no deliberative process/privileged materials are involved, records contain no (or limited) personal privacy information/did not come from Privacy Act systems of records concerning other individuals, or time extensions not anticipated.

(c) Complex requests will take substantial time, will cause significant impact on responding units. Complications and delays are likely. Records sought are massive in volume, multiple organizations must review/coordinate on records, records are classified, records originated with a nongovernment source, records were part of the Air Force's decision-making process or are privileged.

(d) Expedited processing. Examples of letters to individuals whose FOIA requests and/or appeals were not expedited are included in §806.27.

### §806.7 Use of exemptions.

(a) A listing of some AFIs that provide guidance on special disclosure procedures for certain types of records is provided in §806.28. Refer to those instructions for specific disclosure procedures. Remember, the only reason to deny a request is a FOIA exemption.

(b) Refer requests from foreign government officials that do not cite the FOIA to your foreign disclosure office and notify the requester.

(c) If you have a non-U.S. Government record, determine if you need to consult with the record's originator before releasing it (see §806.9 and §806.15(c)). This includes records created by foreign governments and organizations such as North Atlantic Treaty Organization (NATO) and North American Aerospace Defense (NORAD). You may need to coordinate release of foreign government records with either the U.S. Department of State or with the specific foreign embassy, directly

through the MAJCOM FOIA office. Coordinate release or denial of letters of offer and acceptance (LOA) with SAF/IA through 11 CS/SCSR (FOIA), 1000 Air Force Pentagon, Washington DC 20330-1000.

### §806.8 Description of requested record.

Air Force elements must make reasonable efforts to find the records described in FOIA requests. Reasonable efforts means searching all activities and locations most likely to have the records, and includes staged or retired records, as well as complete and thorough searches of relevant electronic records, such as databases, word processing, and electronic mail files.

### §806.9 Referrals.

(a) Send all referrals through the FOIA office. The receiving FOIA office must agree to accept the referral before transfer. The FOIA office will provide the name, phone number, mailing address, and e-mail address of both the FOIA office point of contact and the record OPR point of contact in their referral letter. Include the requested record. If the requested records are massive, then provide a description of them. Referrals to, or consultations with, DFOISR are accomplished from the MAJCOM level. Section 806.27 has an example of a referral memo.

(b) In some cases, requested records are available from the GPO and NTIS, 5285 Port Royal Road, Springfield VA 22161. These organizations offer certain records for sale to the public. Current standard releasable Air Force publications are available electronically on the WWW at <http://afpubs.hq.af.mil/>. For requesters without electronic access, NTIS has paper copies for sale. Give requesters the web address or NTIS address when appropriate. However, if the requester prefers to pursue the FOIA process, consult with HQ AFCIC/ITC through the MAJCOM. Refer FOIA requests for Air Force publications that are classified, FOUO, rescinded, or superseded to the OPR through the appropriate FOIA office.

### §806.10 Records management.

Keep records that were fully released for 2 years and denied records for 6

years. Include in the 6-year record file copies of records or parts of records that were released in response to the same request. Refer to Air Force Manual (AFMAN) 37-139, Records Disposition Schedule (converting to AFMAN 33-339, see § 806.9(b)). The functional OPR or FOIA office may keep the records released or denied. The FOIA office keeps the FOIA case file for each request. The FOIA case file consists of: the initial request; tasking to OPRs; OPR's reply; memoranda for record (MFR) of phone calls or other actions related to the FOIA request; DD Forms 2086, Record of Freedom of Information (FOI) Processing Cost, or 2086-1, Record of Freedom of Information (FOI) Processing Cost for Technical Data; final response; and any of the following, if applicable: extension letter; legal opinions; submitter notification letters and replies; the appeal and required attachments (except for the released or denied records if maintained by the OPR); and all other correspondence to and from the requester.

**§ 806.11 FOIA reading rooms.**

Each FOIA office will arrange for a reading room where the public may inspect releasable records. You do not need to co-locate the reading room with the FOIA office. The FOIA does not require creation of a reading room dedicated exclusively to this purpose. A "reading room" is any location where a requester may review records. For FOIA-processed (a)(3) records, if requesters meet the criteria for search and review costs, they must be paid before inspecting records. Assess reproduction costs at the time of inspection, if appropriate.

**§ 806.12 Record availability.**

(a) HQ AFCIC/ITC will make the traditional FOIA-processed (a)(2) materials (5 U.S.C. 552(a)(2)(A), (B), and (C)) available to the public. Each Air Force activity must make 5 U.S.C. 552(a)(2)(D) records ("FOIA-processed (a)(2)(D) records"—records which they determine will, or have become, the subject of frequent or subsequent requests) available to the public in a reading room in hard copy and electronically by posting it to their appropriate web site. There is no require-

ment to make all FOIA-released records available electronically. The FOIA manager, in coordination with the functional OPR, or the owner of the records, determines qualifying records, after coordination with any interested OCRs. As required by AFIs 33-129 and 35-205, OPRs request clearance of these records with the PAO before posting on the WWW.

(b) Normally, if the FOIA office or OPR receives, or anticipates receiving, five or more requests for the same record in a quarter, they will consider it a frequently requested record (FOIA-processed (a)(2)(D) record) and make it publicly available in hard copy and electronically as outlined in § 806.12(a). OPRs may elect to make other records publicly available if they receive, or expect to receive, less than five requests a quarter. The purpose is to make records available in an ERR to potential future FOIA requesters instead of waiting to receive a FOIA request, and reduce the number of multiple FOIA requests for the same records requiring separate responses. In making these determinations, recognize there are some situations in which a certain type of record becomes the subject of simultaneous FOIA requests from all interested parties and then ceases to be of interest. Activities may typically receive a "flurry" of FOIA requests for contract records immediately after a contract is awarded, but do not receive any subsequent requests for such bulky records after that point. In some cases, activities may decide that placing records in the ERR would not serve the statutory purpose of "diverting some potential FOIA requests for previously released records." The following types of records should be considered for inclusion in the ERR (excluding individuals assigned to overseas, sensitive, and routinely deployable units): organizational charts and limited staff directories; lists of personnel reassigned with gaining base; MAJCOM FOIA supplements; lists of International Merchant Purchase Authority Card (IMPAC) card holders. Do not post lists of e-mail addresses.

(c) GILS. Each activity that posts FOIA-processed (a)(2)(D) records (records which they determine will, or

have become, the subject of frequent or subsequent requests) must create a GILS record for each FOIA-processed (a)(2)(D) record and post it to DefenseLINK. The OPR prepares the GILS record. You can complete and submit a GILS record on-line using a web browser. Instructions for completing the GILS record, and an on-line form are at <http://www.defenselink.mil/locator/index.html>. Follow the steps listed on the web page. The GILS site on DefenseLINK will serve as the central index of Air Force FOIA-processed (a)(2)(D) records.

(d) In addition, installations will post a list, or index, of locally produced FOIA-processed (a)(2)(D) records on their web page at their FOIA site. Each listing will point or link to the particular record. In addition, MAJCOMs may choose to post their own index of MAJCOM specific FOIA-processed (a)(2)(D) records to their appropriate web site. Installation web pages will include the following phrase (or similar words) on their FOIA site if they do not have any frequently requested FOIA records: "There are no frequently requested FOIA records to post at this time." Include the following statement, or a similar one, on the installation web page with the records: "Some records are released to the public under the FOIA, and may therefore reflect deletion of some information in accordance with the FOIA's nine statutory exemptions. A consolidated list of such records is on DefenseLINK." Link the word "DefenseLINK" to [www.defenselink.mil/locator/fpr\\_index.html](http://www.defenselink.mil/locator/fpr_index.html). Qualifying releasable records with exempt information redacted must show on the record the amount of information withheld and the exemption reason (for example, (b)(6)). Activities with such records should provide the public an index and explanation of the FOIA exemptions. All installation FOIA pages will include a link to the Air Force page.

(e) FOIA web pages should be clearly accessed from the main installation page, either by a direct link to "FOIA" or "Freedom of Information Act" from the main page, or found under a logical heading such as "Library" or "Sites."

#### § 806.13 5 U.S.C. 552(a)(2) materials.

The GILS records on DefenseLINK will serve as the index for 5 U.S.C. 552(a)(2)(D) materials.

#### § 806.14 Other materials.

HQ AFCIC/ITC makes the appropriate FOIA-processed (a)(1) materials available for the Air Force.

#### § 806.15 FOIA exemptions.

(a) *Exemption number 1.* When a requester seeks records that are classified, or should be classified, only an initial classification authority, or a declassification authority, can make final determinations with respect to classification issues. The fact that a record is marked with a security classification is not enough to support withholding the document; make sure it is "properly and currently classified." Review the record paragraph by paragraph for releasable information. Review declassified and unclassified parts before release to see if they are exempt by other exemptions. Before releasing a reviewed and declassified document, draw a single black line through all the classification markings so they are still legible and stamp the document unclassified. If the requested records are "properly and currently classified," and the Air Force withholds from release under FOIA exemption (b)(1), and the requester appeals the withholding, include a written statement from an initial classification authority or declassification authority certifying the data was properly classified originally and that it remains properly classified per Executive Order. Examples of initial classification and declassification authority statements are included in § 806.27. Guidance on document declassification reviews is in AFI 31-401, Managing the Information Security Program, and DoD 5200.1-R, Information Security Program, January 1997.

(b) *Exemption number 3.* HQ AFCIC/ITC will provide the current FOIA-processed (b)(3) statutes list to the MAJCOMs.

(c) *Exemption number 4.* The Air Force, in compliance with Executive Order 12600, will advise submitters of contractor-submitted records when a FOIA requester seeks the release of such records, regardless of any initial

determination of whether FOIA exemption (b)(4) applies. (See § 806.20(a) and § 806.31). Due to a change to Title 48 CFR, Federal Acquisition Regulations System, submitter notification is not required prior to release of unit prices contained in contracts awarded based upon solicitations issued after January 1, 1998. For solicitations issued before January 1, 1998, conduct a normal submitter notice. Unit prices contained in proposals provided prior to contract award are protected from release, as are all portions of unsuccessful proposals (before and after contract award) (10 U.S.C. 2305(g), Prohibition on Release of Contractor Proposals).

(d) *Exemption number 5.* (1) Attorney-client records could include, e.g., when a commander expresses concerns in confidence to his or her judge advocate and asks for a legal opinion. The legal opinion and everything the commander tells the judge advocate in confidence qualify under this privilege. Unlike deliberative process privilege, both facts and opinions qualify under the attorney work product or attorney-client privilege. Attorney work product records are records an attorney prepares, or supervises the preparation of, in contemplating or preparing for administrative proceedings or litigation.

(2) Based on court decisions in FOIA litigation, which led to the release of results of personnel surveys, FOIA managers and IDAs should get advice from an Air Force attorney before withholding survey results under FOIA exemption (b)(5).

(e) *Exemption number 6.* (1) AFI 37-132, Air Force Privacy Act Program (will convert to AFI 33-332) provides guidance on collecting and safeguarding social security numbers (SSN). It states: "SSNs are personal and unique to each individual. Protect them as FOUO. Do not disclose them to anyone without an official need to know." Before releasing an Air Force record to a FOIA requester, delete SSNs that belong to anyone other than the requester. In any subsequent FOIA release to a different requester of those same records, make sure SSNs are deleted. When feasible, notify Air Force employees when someone submits a FOIA request for information about them. The notification letter should include a brief de-

scription of the records requested. Also include a statement that only releasable records will be provided and we will protect personal information as required by the FOIA and Privacy laws.

(2) Personal information may not be posted at publicly accessible DoD web sites unless to do so is clearly authorized by law and implementing regulation and policy. Personal information should not be posted at nonpublicly accessible web sites unless it is mission essential and appropriate safeguards have been established. See also AFIs 33-129 and 35-205.

(3) Withhold names and duty addresses of personnel serving overseas or in sensitive or routinely deployable units. Routinely deployable units normally leave their permanent home stations on a periodic or rotating basis for peacetime operations or for scheduled training exercises conducted outside the United States or United States territories. Units based in the United States for a long time, such as those in extensive training or maintenance activities, do not qualify during that period. Units designated for deployment on contingency plans not yet executed and units that seldom leave the United States or United States territories (e.g., annually or semiannually) are not routinely deployable units. However, units alerted for deployment outside the United States or United States territories during actual execution of a contingency plan or in support of a crisis operation qualify. The way the Air Force deploys units makes it difficult to determine when a unit that has part of its personnel deployed becomes eligible for denial. The Air Force may consider a unit deployed on a routine basis or deployed fully overseas when 30 percent of its personnel have been either alerted or actually deployed. In this context, alerted means that a unit has received an official written warning of an impending operational mission outside the United States or United States territories. Sensitive units are those involved in special activities or classified missions, including, for example, intelligence-gathering units that collect, handle, dispose of, or store classified information and materials, as well as units that train or advise foreign personnel.

(i) Each MAJCOM and FOA will establish a system and assign OPRs to identify United States-based units in their command qualifying for the "sensitive or routinely deployable unit" designation, under this exemption. Appropriate OPRs could include directors of operations, plans and programs, and personnel.

(ii) MAJCOM FOIA managers will ensure the list of sensitive and routinely deployable units is reviewed in January and July, and will follow that review with a memo to the Air Force Personnel Center (HQ AFPC/MSIMD), 550 C Street West, Suite 48, Randolph AFB, TX 78150-4750, either validating the current list or providing a revised listing based on the current status of deployed units at that time. This listing is in American Standard Code for Information Interchange (ASCII) format on a 3½" (double-sided, high-density) diskette, which contains the unit's eight-position personnel accounting symbol (PAS) code, with one PAS code per line (record) (8-byte record). The MAJCOM FOIA manager will send an electronic copy of the list of nonreleasable units to HQ AFPC/MSIMD which is included in the personnel data system. The MAJCOM and HQ AFPC FOIA offices will use it to determine releasable lists of names and duty addresses. This reporting requirement is exempt from licensing with a reports control symbol (RCS) in accordance with AFI 37-124, The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections (will convert to AFI 33-324).

(f) *Exemption number 7.* Guidance provided in §806.15(e)(1) also applies to SSNs in records compiled for law enforcement purposes. Do not disclose SSNs to anyone without an official need to know.

#### § 806.16 For official use only.

(a) Markings. Record owners may also add the following sentence to the statement above: "(Further distribution is prohibited without the approval of (owner's organization, office symbol, phone).)"

(b) Dissemination and transmission.  
(1) When deciding whether to send

FOUO records over facsimile equipment, balance the sensitivity of the records against the risk of disclosure. When faxing, use cover sheets to indicate FOUO attachments (*i.e.*, AF Form 3227, Privacy Act Cover Sheet, for Privacy Act information). Consider the location of sending and receiving machines and ensure authorized personnel are available to receive FOUO information as soon as it is transmitted.

(2) For Privacy Act records, refer to AFI 33-332 for specific disclosure rules. For releases to GAO and Congress, refer to AFI 90-401, Air Force Relations With Congress and AFI 65-401, Relations With the General Accounting Office. See §806.9(b) for availability.

(c) Termination, disposal and unauthorized disclosures. You may recycle FOUO material. Safeguard the FOUO documents or information to prevent unauthorized disclosure until recycling. Recycling contracts must include specific responsibilities and requirements on protecting and destroying FOUO and Privacy Act materials.

#### § 806.17 Release and processing procedures.

(a) Individuals seeking Air Force information should address requests to an address listed in §806.26. MAJCOM FOIA office phone numbers and mailing addresses are available on the Air Force FOIA Web Page at <http://www.foia.af.mil>.

(1) A list of Air Force FOIA processing steps, from receipt of the request through the final disposition of an administrative appeal is at §806.29, which also includes guidance on preparing and processing an Air Force FOIA appeal package.

(2) Air Force host tenant relationships. The Air Force host base FOIA manager may log, process, and report FOIA requests for Air Force tenant units. In such cases, the host base FOIA office refers all recommended denials and "no records" appeals to the Air Force tenant MAJCOM FOIA manager. This does not apply to the Air National Guard (ANG), Air Force Reserves, or to disclosure authorities for specialized records.

(b) Use FOIA procedures in this part to process any congressional request citing FOIA, or covering a constituent

## § 806.18

letter citing FOIA. This does not apply to requests from a Congressional Committee or Subcommittee Chair on behalf of the committee or subcommittee.

### § 806.18 Initial determinations.

(a) Disclosure authorities make final decisions on providing releasable records within the time limits and provide recommendations to the IDA on proposed denials and partial denials after coordination with the appropriate FOIA and JA office. Normally, disclosure authorities are division chiefs or higher at Air Staff level. MAJCOMs will designate their disclosure authority levels. The level should be high enough so a responsible authority makes the disclosure according to the policies outlined in this part. At out sourced units or functions, the disclosure authority must be a government official. Contractors who are functional OPRs for official government records are not authorized to make the decision to disclose government records.

(b) On receipt, Air Force FOIA offices will promptly inform Air Force PAOs of all FOIA requests that are potentially newsworthy, or that are submitted by news media requesters. FOIA offices will coordinate final replies for such cases with public affairs.

### § 806.19 Reasonably segregable portions.

Delete information exempt from release under the FOIA from copies of otherwise releasable records. Do not release copies that would permit the requester to "read through the marking." Examples of records with deletions of exempted data are in § 806.30.

### § 806.20 Records of non-U.S. government source.

(a) The Air Force, in compliance with Executive Order 12600, will advise submitters of contractor-submitted records when a FOIA requester seeks the release of such records, regardless of any initial determination as to whether FOIA exemption (b)(4) applies. See § 806.15(c) and § 806.31. Due to a change to 48 CFR, submitter notification is not required prior to release of unit prices contained in contracts awarded based upon solicitations

## 32 CFR Ch. VII (7-1-12 Edition)

issued after January 1, 1998. For solicitations issued before January 1, 1998, conduct a normal submitter notice. Unit prices contained in proposals provided prior to contract award are protected from release, as are all portions of unsuccessful proposals (before and after contract award) (10 U.S.C. 2305(g)).

(b) Department of State involvement. Air Force FOIA managers will notify their MAJCOM (or equivalent) FOIA office, in writing, via fax or e-mail when the Department of State becomes involved in any Air Force FOIA actions. The MAJCOM FOIA office will provide 11 CS/SCSR, via fax or e-mail, a summary of the issues involved, and the name, phone number, mailing address and e-mail address of: their own FOIA office point of contact; the Air Force record OPR point of contact, the DoD component FOIA office point of contact (if any), and the Department of State point of contact. 11 CS/SCSR will inform SAF/IA of any State Department involvement in Air Force FOIA actions. (See § 806.7(b).) An example of a memo advising 11 CS/SCSR of State Department involvement in an Air Force FOIA action is provided in § 806.27.

### § 806.21 Appeals.

(a) FOIA requesters seeking Air Force records must address appeals to the Office of the Secretary of the Air Force, through the FOIA office of the IDA that denied the request. Requesters should attach a copy of the denial letter to their appeal and give reasons for appealing. Air Force IDAs may reconsider any prior denials and may grant all or part of a requester's appeal. When any appellate action sought by a FOIA requester is denied by an IDA, the IDA will include a statement that the issues raised in the appeal were considered and rejected (in full or in part) in any file sent to the Secretary of the Air Force in the course of a FOIA appeal action. Send all appeals to IDA decisions at the wing level through the MAJCOM FOIA office for sending to the Secretary of the Air Force's designated appellate authority, SAF/GCA (and Air Force Legal Services Agency (AFLSA/JACL)). (See

## Department of the Air Force, DoD

## § 806.25

§§ 806.4(g), 806.5(b), and § 806.5(k.) Additional steps are required prior to sending an appeal file.

(1) MAJCOM FOIA offices and record OPRs are responsible for ensuring adequate preparation of the FOIA appeal package for reconsideration by the IDA. FOIA offices and records OPRs will coordinate with Air Force attorneys, who will provide written opinions on substantive issues raised in the appeal.

(2) If a requester appeals an Air Force “no records” determination, Air Force elements must search again or verify the adequacy of their first search. The package must include documents that show the Air Force element systematically tried to find responsive records. Tell, for example, what areas or offices were searched and how the search was conducted—manually, by computer, by telephone, and so forth. In the event a requester sues the Air Force to contest a determination that no responsive records exist, formal affidavits are required to support the adequacy of any searches conducted.

(3) FOIA requesters seeking to appeal denials involving Office of Personnel Management’s controlled civilian personnel records must appeal to the Office of the General Counsel, Office of Personnel Management, 1900 E Street NW, Washington, DC 20415.

(4) If a requester appeals a denial of a fee waiver, fee estimate, or fee reduction request, FOIA offices and record OPRs must account for actual and estimated costs of processing a request, and will include copies of the DD Forms 2086 or 2086-1 in the appeal package.

(5) When any appellate action sought by a FOIA requester is denied by an IDA, prepare the FOIA appeal package as specified in § 806.29, and then the MAJCOM FOIA office forwards the appeal file to the Secretary of the Air Force’s designated appellate authority, SAF/GCA (through AFLSA/JACL), for a final administrative determination.

(b) Air Force activities will process appeal actions expeditiously to ensure they reach the Office of the Secretary of the Air Force in a timely manner.

### § 806.22 Time limits.

Any FOIA appeals received after the 60-day time limit are not processed, unless the requester provides adequate justification for failing to comply with the time limit. If a late appeal is received, and there is no adequate justification for failing to comply with the time limit, the FOIA office will advise the FOIA requester their appeal has been closed. An example of a closure letter is included in § 806.27.

### § 806.23 Delay in responding to an appeal.

For an appeal in process and not yet forwarded to AFLSA/JACL, the MAJCOM FOIA office is responsible for advising the requester of the status of the appeal. For an appeal in process at AFLSA/JACL, that office will advise the requester regarding status of the appeal.

### § 806.24 Fee restrictions.

For FOIA purposes, Air Force activities will consider the cost of collecting a fee to be \$15 and will not assess requesters’ fees for any amount less than \$15.

### § 806.25 Annual report.

(a) MAJCOM FOIA managers and AFLSA/JACL send a consolidated report for the fiscal year on DD Form 2564, Annual Report Freedom of Information Act, to HQ AFCIC/ITC by October 30 via regular mail, e-mail, or facsimile. AFLSA/JACL will prepare the appeals and litigation costs sections of the report. HQ AFCIC/ITC will make the Air Force report available on the WWW.

(b) Total requests processed. “Processed” includes responses that give an estimated cost for providing the records, even if the requester has not paid.

(c) Denied in full. Do not report “no record” responses as denials.

(d) Other reasons.

(1) *Referrals*. Also include referrals within Air Force in this category.

(2) *Not an agency record*. The “not an agency record” other reason category only applies to requests for: objects or articles such as structures, furniture, vehicles and equipment, whatever their historical value, or value as evidence;

**§ 806.26**

**32 CFR Ch. VII (7-1-12 Edition)**

anything that is not a tangible or documentary record such as an individual's memory or oral communication; and personal records of an individual not subject to agency creation or retention requirements, created and maintained primarily for the convenience of an agency employee and not distributed to other agency employees for their official use. This category does not include "no record" responses.

(e) Other. The "Other (Specify)" block must contain the reason with the total number for the reason. For example: "FOIA request had no return address-4."

(f) 5 U.S.C. 552(b)(3) statutes invoked on initial determinations. A corresponding statute is required for each instance entered in the Exemption 3 block. List the statute by number, not title. For any statute on the report that is not on DoD's list of commonly used 5 U.S.C. 552(b)(3) statutes, attach a copy of the pertinent page of the statute that states information must be withheld from public disclosure. HQ AFCIC/ITC makes the DoD list available to FOIA managers electronically. Statutes on the DoD list with an asterisk indicate they are valid 5 U.S.C. 552(b)(3) statutes from litigation. Do not enter any of the following as 5 U.S.C. 552(b)(3) statutes:

5 U.S.C. 552  
5 U.S.C. 552a  
28 U.S.C. 1498  
17 U.S.C. 101  
18 U.S.C. 1905.

(g) Appeal determinations. Enter the total number of FOIA appeals received and total number of FOIA appeals completed during the fiscal year.

(h) Average. Air Force will use the "median age" and will not collect or report averages.

(i) Number of initial requests received during the fiscal year. This number includes open and closed cases.

(j) Total number of initial requests. "Processed" includes responses which give an estimated cost for providing the records, even if the requester has not paid.

(k) Total program cost. This figure includes all costs from the DD Forms 2086 and 2086-1, as well as personnel costs for individuals primarily involved in administering the FOIA program. To

figure personnel costs, multiply the annual salary of each person by the percentage of time spent on FOIA.

(l) MAJCOMs and bases do not include the 25 percent. HQ AFCIC/ITC will add to the final Air Force report to DoD.

(m) Authentication. MAJCOM SCs will sign as approving official (or two-letter functional equivalent for FOIA offices in other functional areas).

**§ 806.26 Addressing FOIA requests.**

(a) FOIA requests concerning Air National Guard Inspector General records should be sent to 11 CS/SCSR (FOIA), 1000 Air Force Pentagon, Washington, DC 20330-1000.

(b) Addressing Air Force Freedom of Information Act requests. The Department of the Air Force, a component of the DoD, includes the Office of the Secretary of the Air Force, the Chief of Staff of the Air Force (who is supported by Headquarters Air Force or "Air Staff" elements), the MAJCOMs, the FOAs, and DRUs. This section lists the FOIA office addresses. A selected subordinate unit is also included in this section. Realignment of Air Force elements is frequent; addresses listed below are subject to change.

(c) The Department of the Air Force does not have a central repository for Air Force records. FOIA requests are addressed to the Air Force element that has custody of the record desired. In answering inquiries regarding FOIA requests, Air Force personnel will assist requesters in determining the correct Air Force element to address their requests. If there is uncertainty as to the ownership of the record desired, refer the requester to the Air Force element that is most likely to have the record. Two organizations that include Air Force elements, and hold some Air Force-related records, are also included in the addresses listed below.

(d) MAJCOMs:

(1) Air Combat Command (ACC): HQ ACC/SCTC, 230 East Flight Line Road, Langley AFB VA 23665-2781.

(2) Air Education and Training Command (AETC): HQ AETC/SCTS, 61 Main Circle Suite 2, Randolph AFB TX 78150-4545.

## Department of the Air Force, DoD

§ 806.26

(3) Air Force Materiel Command (AFMC): HQ AFMC/SCDP, 4225 Logistics Avenue, Suite 6, Wright-Patterson AFB, OH 45433-5745.

(4) Air Force Reserve Command (AFRC): HQ AFRC/SCSM, 155 2nd Street, Robins AFB, GA 31098-1635.

(5) Air Force Special Operations Command (AFSOC): HQ AFSOC/SCMN, 100 Bartley Street, Suite 201, Hurlburt Field, FL 32544-5273.

(6) Air Force Space Command (AFSPC): HQ AFSPC/SCMA, 150 Vandenberg Street, Suite 1105, Peterson AFB, CO 80914-4400.

(7) Air Mobility Command (AMC): HQ AMC/SCYNR, 203 West Losey Street, Room 3180, Scott AFB, IL 62225-5223.

(8) Pacific Air Forces (PACAF): HQ PACAF/SCT, 25 E Street, Suite C220, Hickam AFB, HI 96853-5409.

(9) United States Air Forces in Europe (USAFE): HQ USAFE/SCMI, Unit 3050, Box 125, APO AE 09094-0125.

### (e) FOAs:

(1) Air Force Audit Agency (AFAA): HQ AFAA/IMP, 1126 Air Force Pentagon, Washington, DC 20330-1126.

(2) Air Force Base Conversion Agency (AFBCA): AFBCA/ESA, 1700 North Moore Street, Suite 2300, Arlington, VA 22209-2802.

(3) Air Force Center for Environmental Excellence (AFCEE): HQ AFCEE/MSI, 3207 North Road, Brooks AFB, TX 78235-5363.

(4) Air Force Civil Engineering Support Agency (AFCESA): HQ AFCESA/IMD, 139 Barnes Drive Suite 1, Tyndall AFB, FL 32403-5319.

(5) Air Force Historical Research Agency (AFHRA): AFHRA/RSA, 600 Chennault Circle, Maxwell AFB, AL 36112-6424.

(6) Air Force Inspection Agency (AFIA): (Shared FOIA office/function, AFIA and Air Force Safety Agency) AFSA/JAR, 9700 Avenue G SE, Suite 236B, Kirtland AFB, NM 87117-5670.

(7) Air Force Medical Support Agency (AFMSA): AFMSA/CCEA, 2510 Kennedy Circle, Suite 208, Brooks AFB, TX 78235-5121.

(8) Air Force News Agency (AFNEWS): HQ AFNEWS/SCB, 203 Norton Street, Kelly AFB, TX 78241-6105.

(9) Air Force Office of Special Investigations (AFOSI): HQ AFOSI/SCR, P. O. Box 2218, Waldorf, MD 20604-2218.

(10) Air Force Personnel Center (AFPC): HQ AFPC/MSIMD, 550 C Street West, Suite 48, Randolph AFB, TX 78150-4750.

(11) Air Force Center for Quality and Innovation (AFCQMI): AFCQMI/CSP, 550 E Street East, Randolph AFB, TX 78150-4451.

(12) Air Force Safety Agency (AFSA): (Shared FOIA office/function, AFIA, and AFSA) AFSA/JARF, 9700 Avenue G SE, Suite 236B, Kirtland AFB, NM 87117-5670.

(13) Air Force Security Forces Center (AFSFC): AFSFC/CCQ 1720 Patrick Street, Lackland AFB, TX 78236-5226.

(14) Air Force Services Agency (AFSVA): AFSVA/SVSR, 9504 1H-35 North, Suite 250, San Antonio, TX 78233-6635.

(15) Air Force Technical Applications Center (AFTAC): AFTAC/LSCS, 1030 South Highway, Suite A1A, Patrick AFB, FL 32925-6001.

(16) Air Intelligence Agency (AIA): AIA/DOOI, 102 Hall Boulevard, Suite 229, San Antonio, TX 78243-7029.

(17) Air Reserve Personnel Center (ARPC): ARPC/SCS, 6760 East Irvington Place, #6600, Denver, CO 80280-6600.

(18) Air Force Weather Agency (AFWA): HQ AFWA/SCI, 106 Peacekeeper Drive Suite 2N3, Offutt AFB, NE 68113-4039.

(19) Air Force History Support Office (AFHSO): AFHSO, 500 Duncan Avenue Box 94, Bolling AFB, DC 20332-1111.

### (f) DRUs:

(1) Air Force Operational Test and Evaluation Center (AFOTEC): AFOTEC/SCM, 8500 Gibson Boulevard SE, Kirtland AFB, NM 87117-5558.

(2) 11th Wing: 11 CS/SCSR (FOIA), 1000 Air Force Pentagon, Washington, DC 20330-1000 (if a person is unsure where to send a FOIA request for Air Force records, or is seeking records from the Office of the Secretary of the Air Force, or other Headquarters Air Force records, use this address).

(3) United States Air Force Academy (USAFA): 10 CS/SCBD, 2304 Cadet Drive, Suite 232, USAFA, CO 80840-5060.

(g) Selected subordinate units: Air Force Communications Agency (AFCA): HQ AFCA/CCQI, 203 West Losey Street, Room 1022, Scott AFB, IL 62225-5203.

**§ 806.27**

**32 CFR Ch. VII (7-1-12 Edition)**

(h) Organizations which include air force elements:

(1) Army and Air Force Exchange Service (AAFES): HQ AAFES/GC-E, P.O. Box 660202, Dallas, TX 75266-0202.

(2) National Guard Bureau (NGB)/Air National Guard: NGB-AD, 2500 Army Pentagon, Washington, DC 20310-2500. (FOIA requests concerning Air National Guard IG records should be sent to 11 CS/SCSR (FOIA), 1000 Air Force Pentagon, Washington, DC 20330-1000)

**§ 806.27 Samples of Air Force FOIA processing documents.**

(a) This section includes suggested language in paragraph format that tracks Air Force and DoD FOIA guidance. The rest of the body of letters and memorandums should comply with Air Force administrative guidance. Each MAJCOM may elect to prepare their own verbiage to meet their specific needs, so long as FOIA processing actions are consistent with guidance in DoD 5400.7-R and this part. In this section, language in parentheses is for explanatory purposes only. Do not include any of the parenthetical language of this section in your FOIA correspondence. When optional language must be selected, the optional language will be presented within parentheses. Use only the portions that apply to the specific request or response.

(b) Initial receipt of Freedom of Information Act request.

We received your Freedom of Information Act (FOIA) request dated ## Month year, for (summarize the request) on ## Month year (date received). We will provide you our release determination by (enter date that is 20 workdays from date you received the request). (Based on our initial review, we believe we cannot process your request within 20 workdays.) (If "cannot" is used, add appropriate explanation; examples follow.) Please contact (name and commercial telephone number) if you have any questions and refer to case number #####.

(c) Interim response:

Your request will be delayed because: all or part of the responsive records are not located at this installation; (and/or) Processing this FOIA request will require us to collect and review a substantial number of records (and/or) Other Air Force activities or other agencies (if applicable) to include the submitter of the information, need to be involved in deciding whether or not to release the respon-

sive records. We expect to reply to your request not later than (give a date that is not more than 30 workdays from the initial receipt of the request); (or) If processing the FOIA request will take more than the allowed time limits to respond. We find we are unable to meet the time limits imposed by the FOIA in this instance because (tell the requester the reason for the delay) (example: the records are classified and must be reviewed for possible declassification by other activities or agencies). We anticipate completing your request by (date).

(When charging fees is appropriate.) The FOIA provides for the collection of fees based on the costs of processing a FOIA request and your fee category. Based on the information in your request, we have determined your fee category is (commercial/educational or noncommercial scientific institution or news media/all others). As a result, you (if commercial category) are required to pay all document search, review and duplication costs over \$15.00. (or) As a result, you (if educational or noncommercial scientific institution or news media) will be provided the first 100 pages free of charge; you are required to pay any duplication costs over and above those amounts. (or) As a result, you will be provided the first 2 hours of search time and the first 100 pages free of charge; you are required to pay any search and duplication costs over and above those amounts.

(d) Request for a more specific description:

Your request does not sufficiently describe the desired records. The FOIA applies to existing Air Force records; without more specific information from you, we cannot identify what documents might be responsive to your request. Please give us whatever additional details you may have on the Air Force records you want. Can you tell us when the records were created, and what Air Force element may have created the records? If this request involves an Air Force contract, do you know the contract number and dates it covered? Our address is (include name and complete mailing address), our fax number is (give fax number), our e-mail address is (optional—give complete e-mail address). Based on the original request you sent us, we are unable to respond.

(e) Single letter acknowledging receipt of request and giving final response. (If you can complete a FOIA request within the statutory 20-workday processing period, Air Force elements may elect to send a single letter to the requester, along with responsive records which are released to the requester in full).

## Department of the Air Force, DoD

## § 806.27

We received your Freedom of Information Act (FOIA) request dated ## Month year, for (summarize the request) on ## Month year (date received). A copy (or) Copies of (describe the record(s) being released) (is/are) releasable and (is/are) attached.

### (f) Collection of fees:

The FOIA provides for the collection of fees based on the costs of processing a FOIA request and your fee category. We have placed you in the (enter the fee category) fee category. In your case, we have assessed a charge of \$ \_\_\_ for processing your request. The fee was calculated in the following manner: (Give a detailed cost breakdown: for example, 15 pages of reproduction at \$0.15 per page; 5 minutes of computer search time at \$43.50 per minute, 2 hours of professional level search at \$25 per hour.) Please make your check payable to (appropriate payee) and send it to (give your complete mailing address) by (date 30 days after the letter is signed). (or) The FOIA provides for the collection of fees based on the costs of processing a FOIA request and your fee category. We have placed you in the (enter the fee category); however, in this case, we have waived collecting fees.

(g) Multitrack processing letters to FOIA requesters. (When using the multitrack FOIA processing system, determine which of the following paragraphs to include in your letters to the requester. To the extent it may apply, include language from paragraph 2 of the sample. If a requester asks for expedited processing, answer carefully if you decide not to provide expedited processing, because requesters may appeal denial of their request for expedited processing. Advise requesters placed into the complex track in writing how they can simplify their request to qualify for the simple track.)

We received your Freedom of Information Act (FOIA) request dated ## Month year, for (summarize the request) on ## Month year (date received). Because our organization has a significant number of pending FOIA requests, which prevents us from making a response determination within 20 workdays, we have instituted multitrack processing of requests. Based on the information you provided, we have placed your request in the (simple or complex) track. We have assigned number ##### to identify your request; should you need to contact us about your request, please write or call (name and telephone) and use this number to assist us in responding more promptly.

Based on our current backlog, we expect to respond to your request not later than (give

an estimated date). Our policy is to process requests within their respective tracks in the order in which we receive them. We do process each FOIA request as quickly as we can.

(h) If the request is placed in the complex track:

In your case, processing your request is complex because (give basic reasons this is a complex case: request was vague or complicated; the records sought are voluminous; multiple organizations will have to work on this request; records are classified; responsive records came from another command/another service/a nongovernment source; responsive records were part of the Air Force's decision-making process, and the prerelease review will require policy determinations from different Air Force elements; records describe law enforcement activities; records involve foreign policy issues; due to the nature of your request and/or the nature of our computer system, responding to your request or providing a response in the electronic format you requested will be technically complex, etc.). Simplifying your request might permit quicker processing in the following ways: (describe ways the search could be narrowed to fewer records, or ways policy issues could be avoided, etc.) Can you tell us when the records were created, and what Air Force element may have created the records? If this request involves an Air Force contract, do you know the contract number? Please give us whatever additional details you may have on the Air Force records you are seeking, so we can attempt to streamline the processing of your request. Our address is (give complete mailing address), our fax number is (give fax number), our e-mail address is (optional—give complete e-mail address).

(i) If the requester asks that you expedite their request:

Because individuals receiving expedited processing may receive a response before other earlier requesters, there are administrative requirements you must meet before we can expedite a request. In your request, you asked that we expedite processing. In order for us to expedite a request, the requester must provide a statement certifying the reasons supporting their request are true and correct to the best of their knowledge.

In the second category, "urgently needed" means the information itself has a particular value that it will lose if it is not disseminated quickly. Ordinarily this means the information concerns a breaking news story of general public interest. Historic information, or information sought for litigation or commercial activities usually would not

qualify for expedited processing in the second category. Also, the fact that a news organization has an internal broadcast or publication deadline, so long as the deadline was unrelated to the nature of the information itself (for example, the information was not a breaking news story of general public interest) would not make the information “urgently needed.”

In this case, we have determined your FOIA request (will/will not) receive expedited processing. We came to this conclusion because you (did/did not) demonstrate you need the information because failure to obtain the records on an expedited basis (could or could not) reasonably expect to pose an imminent threat to life or physical safety of an individual (or) the information (is or is not) urgently needed in order to inform the public about actual or alleged Federal Government activity (or) failure to obtain the records on an expedited basis (could or could not) reasonably expect to lead to an imminent loss of substantial due process rights, (or) release (would or would not) serve a humanitarian need by promoting the welfare and interests of mankind (and/or) your request for expedited processing did not meet the statutory requirements of the FOIA; you did not provide enough information to make a determination of compelling need for the information you requested (and/or) you did not properly certify your request.

(j) If you deny a request for expedited processing:

If you consider our decision not to expedite your request incorrect, you may appeal our decision. Include in your appeal letter the reasons for reconsidering your request for expedited processing, and attach a copy of this letter. Address your appeal to Secretary of the Air Force through (address of MAJCOM FOIA office). In the meantime, we will continue to process your request in the (simple/complex) processing track.

(k) Certification, computer systems manager (electronic records or format requested).

(When answering a request for electronic records, based on the configuration of your hardware and/or software, certain factors may make a particular request complex. Have your computer system manager advise you whether or not they can create the new record/format on a “business as usual” basis. If producing the record/format would entail a significant expenditure of resources in time and manpower that would cause significant interference with the operation of the information system and adversely affect mission accomplishment, you do not need to process the request. The FOIA office needs to get a certification from the computer systems manager to document this determination to

support their response. Possible language for this certification is provided below.)

I, (rank/grade and name) am the computer systems manager for (organization with electronic records responsive to FOIA request). In consultation with (FOIA office), I have considered the FOIA request of (requester’s name), our ##### (FOIA identifier), which asked for (describe electronic record or format). We (do/do not) have electronic records that are responsive to this request (or) data that we (can/cannot) configure into the requested format. (If there are electronic records) The existing electronic records (do/do not) contain nonreleasable data that we (can/cannot) remove from the electronic record. Because of the way our (computer system/database/software) (use all that apply, specify hardware and/or software nomenclature if possible; for example, IBM ###, Microsoft Excel) is configured, creating the electronic record (or) modifying the existing record/format would entail a significant expenditure of resources in time and manpower that would cause significant interference with the operation of the information system and adversely affect mission accomplishment (describe how responding would interfere and time/manpower resources required, give estimated reprogramming time, if possible). I have applied the DoD “standard of reasonableness” in considering this request. I understand that when the capability exists to respond to a FOIA request that would require only a “business as usual” approach to electronically extract the data and compile an electronic record or reformat data to satisfy a FOIA request, then creation of the electronic record or reformatting the data would be appropriate. In this case, a significant expenditure of resources and manpower would be required to compile the electronic record (or) reformat existing data. This activity would cause a significant interference with the operation of our automated information system. I certify creation of the electronic record (or) reformatting existing data in order to respond to this request would not be reasonable, under the circumstances.

Signature

(Date Signed) (Signature Block)

(NOTE: Some electronic data requests may include a request for software. You may have to release government-developed software that is not otherwise exempt, if requested under the FOIA. Exemptions 1—classified software, 2—testing, evaluation, or similar software, 3—exempt by statute, 5—deliberative process/privileged software, and 7—law enforcement operations software may apply, based on the nature of the requested software. If the software is commercial off-the-shelf software, as opposed to software developed by the government, the software may

**Department of the Air Force, DoD**

**§ 806.27**

qualify to be withheld from release under FOIA exemption 4.

(1) "No (paper or electronic) records" or "requested format not available" letters.

This is in response to your Freedom of Information Act (FOIA) request dated ## Month year, for (summarize the request) on ## Month year (date received), our number #####.

A thorough search by (identify the unit(s) that tried to locate responsive records) did not locate any records responsive to your request. (If the requester asked questions, and there are no responsive records that would provide the answers to those questions): The FOIA applies to existing Air Force records; the Air Force need not create a record in order to respond to a request.

(or) A thorough assessment by the OPR and the computer systems manager has determined we cannot provide the (electronic record data) in the format you requested. (If this can be done on a "business as usual basis):" (Paper copies American Standard Code for Information Interchange (ASCII) files) of the data you requested are attached.

If you interpret this "o records" response as an adverse action, you may appeal it in writing to the Secretary of the Air Force. Your appeal should be postmarked no later than 60 calendar days from the date of this letter. Address your letter as follows: Secretary of the Air Force, Thru: (MAJCOM FOIA Office), (mailing address).

The FOIA provides for the collection of fees based on the costs of processing a FOIA request and your fee category. We have placed you in the (enter category) fee category; however, in this case, we have waived fees. (If paper copies or ASCII files are provided:) The FOIA provides for the collection of fees based on the costs of processing a FOIA request and your fee category. In your case, as a requester in the fee category of (add appropriate category), we have assessed a charge of \$ \_\_\_ for processing your request. The fee was calculated in the following manner: (Give a detailed cost breakdown: for example, 15 pages of reproduction at \$0.15 per page; 5 minutes of computer search time at \$43.50 per minute, 2 hours of professional level search at \$25 per hour.) Please make your check payable to (appropriate payee) and send it to (give your complete mailing address) by (date 30 days after the letter is signed).

(m) Referral or coordination letters. (These letters are to tell the requester all or part of the request was referred to another Air Force organization, to refer or coordinate the request to another federal government organization, and to advise a nongovernment sub-

mitter a FOIA request was received for information they submitted.)G56

(1) Letter to requester.

(If all or part of a request has been referred, write to the requester:) Your Freedom of Information Act (FOIA) request dated ## Month year, for (summarize the request) received on ## Month year (date received), our number #####, was referred (or) must be coordinated with (give mailing address of the FOIA office to which you are referring all or part of the request, the identity of the federal government organization you are either coordinating with or are referring all or part of the request to, or that you must coordinate with the nongovernment submitter of responsive information). (On referrals:) That office will process (all/part) of your request (describe which part is being referred if the entire request is not being referred) and they will respond directly to you. (On coordinations:) That organization has a significant interest in the records (or) created the records that may answer to your request. (Before notifying a requester of a referral to another DoD component or federal agency, consult with them to determine if their association with the material is exempt. If so, protect the association and any exempt information without revealing the identity of the protected activity.) (When a nongovernment submitter is involved:) The nongovernment submitter of information that may answer your request needs time to respond to the possible release of information under the FOIA.

Because we must refer (or) coordinate your request outside our organization, your request will be delayed. We will determine whether any records are available; as soon as is practicable, a decision will be made whether to release or to withhold from disclosure any responsive records under the FOIA, 5 U.S.C. 552. Your request will be processed as expeditiously as circumstances permit.

(2) Letter to another government agency.

(If all or part of a request was referred or requires coordination, write to the government entity): On ## Month year (date received), our organization received a Freedom of Information Act (FOIA) request from (identity of requester), Attachment 1, dated ## Month year, for (summarize the request). Based on our assessment of that request, our number #####, we need to (refer/coordinate) (all/part) of that request to you (describe which part is being referred or coordinated, if it was not the entire request). (Name and phone number of person who agreed to the referral or coordination) accepted this referral (or) coordination action was on (date).

## § 806.27

## 32 CFR Ch. VII (7-1-12 Edition)

We notified the requester of this action (see § 806.31).

We (do/do not) hold records responsive to this request. (If do hold is used:) Copies of responsive records located in our files are included at Attachment 3 to assist you in making your assessment on the releasability of (our/your) related records. If you need to contact us, our phone number and address is (give name, phone and complete mailing address), our fax number is (give fax number), our e-mail address is (give complete e-mail address).

(3) Letter to submitter of contract-related information.

(If contractor-submitted information is involved, write to the submitter:) On ## Month year (date received), our organization received a Freedom of Information Act (FOIA) request from (identity of requester), our number #####, dated ## Month year, for (summarize the request). Information you submitted to the Air Force was identified as responsive to this request, see copies attached.

To determine the releasability of the information contained in these documents and to give you the maximum protection under the law, please review the attached documents and give us the information outlined in § 806.31. If you feel the information is privileged or confidential, consists of proprietary commercial or financial information, and otherwise meets the statutory requirements for withholding the information from release under FOIA exemption 4, 5 U.S.C. 552(b)(4), respond to us in writing not later than ## working days from the date of this letter (usually 30 calendar days). If you object to release of this information under the FOIA, identify the items, lines, columns or portions you believe we should withhold from release.

You will also need to provide a written explanation of how release would adversely impact or cause harm to your competitive position, your commercial standing, or other legally protected interests. An assertion that “we should deny because all of the information was submitted in confidence” or “deny because all of the information was marked as proprietary in nature” would not justify withholding of the requested information under the FOIA. If you need to contact us, call or write (give name), phone number is (give commercial number), our address is (give complete mailing address), our fax number is (give fax number), our e-mail address is (give complete e-mail address).

(4) Letter requesting State Department coordination. (If the State Department is involved in coordinating on a request, fax or e-mail 11 CS/SCSR so they can inform SAF/IA if appropriate).

On ## Month year (date received), our organization received a Freedom of Information Act (FOIA) request from (identity of requester), our number #####, dated ## Month year, for (summarize the request). Because of the nature of this request, we were advised by (note the individual and organization who told you to coordinate the request with the State Department; this may be a MAJCOM or Combatant Command—give telephone and facsimile numbers if known) we need to coordinate this request with the Department of State. In accordance with DoD 5400.7-R, Air Force Supplement, we are informing you of their involvement in this FOIA request. (Provide any specifics available.) Air Force records are involved in this action. If you need to contact us, our phone number is (give commercial and DSN numbers), our address is (give complete mailing address), our fax number is (give fax number), our e-mail address is (give complete e-mail address).

(n) Certification of initial classification or declassification authority (When denying a FOIA request, in whole or in part, because the information requested is classified, the initial classification authority, his or her successor, or a declassification authority, needs to determine if the records are “properly and currently classified,” and therefore must be withheld from release under FOIA exemption (b)(1); also, you need to determine that you cannot release any reasonably segregable additional portions. Language that certifies such a determination was made on a FOIA request involving classified records follows).

(1) Sample certification format—all information remains classified.

I, (rank/grade and name) am the initial classification authority (or) the successor to the original initial classification authority (or) the declassification authority for (give an unclassified description of the records concerned). In consultation with (FOIA office), I have assessed the FOIA request of (requester's name), our ##### (FOIA identifier), for records that were properly classified at the time of their creation and currently remain properly classified in accordance with Executive Order (E.O.) 12958, National Security Information, (or) contain information that we have determined is classified in accordance with E.O. 12958 Section 1.5( ) (or) in accordance with E.O. 12958 Section 1.5( ) and is also exempt from declassification in accordance with Section 1.6( ) of the E. O. (or if the record is more than 25 years old) contain information that we have determined is exempt from declassification in accordance with E.O. 12958 Section

Department of the Air Force, DoD

§ 806.28

3.4(b)( ). Unauthorized release could cause (for TOP SECRET, use exceptionally grave; for SECRET use serious; for CONFIDENTIAL do not add language; should read cause damage) damage to national security. There are no reasonably segregable portions that we can release. Consequently release of this information is denied pursuant to 5 U.S.C. 552(b)(1).

Signature

(Date Signed) (Signature Block)

(2) Sample certification format—portions remain classified.

I, (rank/grade and name) am the initial classification authority (or) the successor to the original initial classification authority (or) the declassification authority for (give an unclassified description of the records concerned.) In consultation with (FOIA office), I have assessed the FOIA request of (requester's name), our ##### (FOIA identifier), that asked for records, (or) portions of which were properly classified at the time of their creation. Portions of the records currently remain properly classified in accordance with E.O. 12958. The bracketed information is currently and properly classified in accordance with Section 1.5 (add appropriate subparagraph), E.O. 12958, and is also exempt from declassification in accordance with Section 1.6( ) of the Executive Order (or if the record is more than 25 years old) contain information that we have determined is exempt from declassification in accordance with E.O. 12958 Section 3.4(b)( ). Unauthorized release could cause (for TOP SECRET use exceptionally grave; for SECRET use serious; for CONFIDENTIAL do not add language; should read cause damage) damage to national security. There are no other reasonably segregable portions that we can release. Consequently this information is denied pursuant to 5 U.S.C. 552(b)(1).

Signature

(Date Signed) (Signature Block)

(o) Letter to a requester who has withdrawn their request or appeal. (If a FOIA requester has withdrawn a FOIA request or appeal, sending a final letter to the requester to close the file may be wise. Suggested language to the requester follows):

We received your Freedom of Information Act (FOIA) request (or) appeal dated ## Month year, on ## Month year (date received). After sending us your request (or) appeal, you indicated by (facsimile, letter) that you wished to withdraw your request (or) appeal. We have, therefore, closed your file without further action.

(p) Letter to a requester who has appealed after the 60-day deadline. (We

will not process FOIA appeals received after the 60-day time limit, unless the requester provides adequate justification for failing to comply. If you receive a late appeal, and it gives inadequate justification for failing to comply, the FOIA office will advise the requester their appeal was closed; suggested language for a letter to an untimely requester follows.)

We received your Freedom of Information Act (FOIA) appeal dated ## Month year, on ## Month year (date received). You did not appeal within 60 days of the postmarked date of our denial letter as outlined in our agency regulation. Therefore, we are closing our file.

(q) Letter to a requester who has appealed. (There are occasions when, on reconsideration, an IDA grants all or part of an appeal. When sending their appeal to higher headquarters, notify the requester. Suggested language to a requester who has appealed follows):

We received your Freedom of Information Act (FOIA) appeal, our number #####, dated ## Month year, on ## Month year (date received). We considered the issues raised in your appeal carefully. We have decided to grant (or) partially grant your appeal.

(If you grant all or part of the appeal): Upon reconsideration, we are releasing the requested records (or) granting your request. (If the appeal is only partially granted, describe what portions remain in dispute). (If applicable): We are releasing and attaching all or portions of the responsive records. (If applicable): We will continue processing your appeal for the remaining withheld (records/information).

§ 806.28 Records with special disclosure procedures.

Certain records have special administrative procedures to follow before disclosure. Selected publications that contain such guidance are listed below.

(a) AFI 16-701, Special Access Programs.

(b) AFI 31-206, Security Police Investigations.

(c) AFI 31-501, Personnel Security Program Management.

(d) AFI 31-601, Industrial Security Program Management.

(e) AFI 36-2603, Air Force Board for Correction of Military Records.

(f) AFI 36-2706, Military Equal Opportunity and Treatment Program.

## § 806.29

## 32 CFR Ch. VII (7–1–12 Edition)

(g) AFI 36–2906, Personal Financial Responsibility.

(h) AFI 36–2907, Unfavorable Information File (UIF) Program.

(i) AFI 40–301, Family Advocacy.

(j) AFI 41–210, Patient Administration Functions.

(k) AFI 44–109, Mental Health and Military Law.

(l) AFI 51–201, Administration of Military Justice.

(m) AFI 51–301, Civil Litigation.

(n) AFI 51–303, Intellectual Property—Patents, Patent Related Matters, Trademarks, and Copyrights.

(o) AFI 51–501, Tort Claims.

(p) AFI 51–503, Aircraft, Missile, Nuclear and Space Accident Investigations.

(q) AFI 51–504, Legal Assistance, Notary and Preventive Law Programs.

(r) AFI 51–1102, Cooperation with the Office of the Special Counsel.

(s) AFI 61–204, Disseminating Scientific and Technical Information.

(t) AFI 61–303, Licensing Inventions Made Under Cooperative Research and Development Agreements.

(u) AFI 71–101, Volume 1, Criminal Investigations, and Volume 2, Protective Service Matters.

(v) AFI 84–101, Historical Products, Services, and Requirements.

(w) AFI 90–301, Inspector General Complaints.

(x) AFI 91–204, Safety Investigations and Reports.

### § 806.29 Administrative processing of Air Force FOIA requests.

(a) This section is a checklist format of processing steps and explanations of Air Force and DoD guidance. Each MAJCOM may elect to prepare its own checklists to tailor FOIA processing actions within its own organizations to meet their specific needs, so long as it remains consistent with guidance contained in DoD 5400.7–R, DoD Freedom of Information Act Program, and this part.

(b) Procedures: FOIA requests.

(1) Note the date the request was received, give the request a unique identifier/number, and log the request.

(2) Assess the request to determine initial processing requirements:

(3) Determine what Air Force elements may hold responsive records.

(i) Are responsive records kept at the same or different installations?

(ii) Is referral of (all/part) of the request required?

(4) Determine appropriate processing track (simple/complex/expedited). (Air Force FOIA offices without backlogs do not multitrack FOIA requests.)

NOTE: Requesters have a right to appeal an adverse tracking decision (for example, when it is determined their request will not be expedited). Also, if their request qualifies for the complex track, tell requesters so they may limit the scope of their request in order to qualify for the simple track. FOIA managers must assess a request before placing it into a specific processing track, and must support their actions should the requester appeal. If a request is determined to be complex, or is not expedited when the requester sought expedited processing, you must advise the requester of the adverse tracking decision in writing. See § 806.27 for sample language for this kind of letter to a requester.

(i) Simple. Defines a request that can be processed quickly, with limited impact on the responding units. The request clearly identifies the records, involves no (or few) complicating factors (e.g., there are few or no responsive records, involves only one installation and there are no outside OPRs, involves no classified records (Exemption 1), a law exempts the responsive records from disclosure (Exemption 3), no contractor-submitted records (Exemption 4), no deliberative process/privileged materials (Exemption 5), records contain no (or limited) personal privacy information/did not come from Privacy Act systems of records concerning other individuals (Exemption 6), release of records would have minimal impact on law enforcement (Exemption 7); no time extensions expected, other than the additional 10-workdays allowed in situations outlined in the FOIA). If the requested data must come from electronic records, response can be completed on a “business-as-usual” basis; requires no (or limited) reprogramming of automated information systems and would cause no significant interference with operation of information systems by processing a simple request/providing a response in the electronic format requested.

(ii) Complex. Defines a request whose processing will take substantial time,

will cause significant impact on responding units. Complications and delays are likely (e.g., the request is vague (poor description of records, unclear who or when records were created), records are massive in volume, multiple organizations will receive tasking, records are classified (Exemption 1), records came from another command/service/a nongovernment source (Exemption 4), records are part of the Air Force's decision-making process, and not incorporated into a final decision (IG/audit reports, legal opinions, misconduct or mishap investigations etc.) or are attorney-client records (Exemption 5), records are largely personal information on another individual or came from Privacy Act systems of records (Exemption 6), records describe law enforcement activities or information from (and/or identities of) confidential sources (Exemption 7); response cannot be completed on a "business as usual" basis and would require extensive reprogramming or cause significant interference with operation of the automated information systems. (Advise requester, in writing, of right to limit the scope of their request in order to qualify for simple track.)

(iii) An expedited request is when a requester asks for expedited processing and explains the compelling need (imminent threat to life or physical safety; urgently needed by a person primarily engaged in disseminating information; due process; or humanitarian need) for the requested information. In order to receive expedited processing, requesters must provide a statement certifying their "demonstration" (description) of their specific "compelling need" or due process/humanitarian need is true and correct to the best of their knowledge. When a requester seeks expedited processing, FOIA offices must respond in writing to the requester within 10 calendar days after receipt of the request approving or denying their request for expedited processing. Requesters have a right to appeal an adverse decision (e.g., when it is determined their requests will not be expedited). There are four categories of FOIA requests that qualify for expedited processing:

(A) The requester asserts a "compelling need" for the records, because a failure to obtain records quickly could reasonably be expected to pose an imminent threat to the life or physical safety of an individual.

(B) The requester asserts a "compelling need" for the records, because the information is "urgently needed" by an individual engaged in disseminating information to inform the public (primarily news media requesters; and could also include other persons with the ability to disseminate information).

NOTE: "Urgently needed," in this case, means the information has a particular value that will be lost if it is not disseminated quickly. This normally would apply to a breaking news story of general public interest. Information of historical interest only, or sought for litigation or commercial activities would not qualify, nor would the fact a news media entity had an internal broadcast deadline of its own, which was unrelated to the "news breaking nature" of the information itself, cause the requested information to qualify as "urgently needed."

(C) Failure to obtain records quickly could cause imminent loss of substantial due process rights or providing the information quickly would serve a "humanitarian need" (i.e., disclosing the information will promote the welfare and interests of mankind). While FOIA requests falling into these third and fourth categories can qualify for expedited processing, process them in the expedited track behind the requests qualifying for expedited processing based on "compelling need" (the first two types of expedited FOIA requests).

(5) Determine fee category of requester (commercial/educational—noncommercial scientific institution—news media/all others) and assess fee issues. When all assessable costs are \$15.00 or less, waive fees automatically for all categories of requesters. Assess other fee waiver or reduction requests on a case-by-case basis.

(6) Apply fee waiver/fee reduction criteria in appropriate cases (when requester asks for fee waiver/reduction).

(7) Find the responsive Air Force records (if any).

(i) Send the request to the appropriate OPRs to search for responsive records and to decide whether to recommend release of any responsive

**§ 806.29**

**32 CFR Ch. VII (7-1-12 Edition)**

records. Include a DD Form 2086, Record of Freedom of Information (FOI), or a DD Form 2086-1, Record of Freedom of Information (FOI) Processing Cost for Technical Data, in each request. The OPR must complete and return the appropriate forms and statements to the FOIA office.

(ii) If the OPRs find no responsive records, or if the OPRs desire to withhold any responsive records from release to the requester, the OPRs must provide a written certificate detailing either their unsuccessful search, or their reasons why the documents should be withheld from release under the FOIA; the written OPR statements must accompany the copies of the records the OPR desires to withhold as the FOIA action is processed (e.g., include it in any denial or appeal file).

NOTE: If any part of a FOIA request is denied, and the requester appeals that denial, include all forms, certificates and documents prepared by the OPRs in the FOIA appeal package required in paragraph (d)(5) of this section.

(c) Contacts with FOIA requesters and non-Air Force submitters of data.

(1) Contacts with Air Force elements. A FOIA request is considered "received" (and therefore ready to process) when the FOIA office responsible for processing the request physically receives it, when the requester states a willingness to pay fees set for the appropriate fee category, or, if applicable, when the requester has paid any past FOIA debts and has reasonably described the requested records. Keep hard/paper copies of all memoranda documenting requester contacts with Air Force elements regarding a pending FOIA request in the requester's FOIA file. If the requester contacts Air Force elements telephonically about a pending FOIA request, the Air Force member participating in the conversation must prepare notes or memorandums for record (MFR), and keep those notes or MFRs in the requester's FOIA file. If any part of a FOIA request is denied, and the requester appeals that denial, submit documentation of requester contacts with Air Force elements in chronological order in the FOIA appeal package (see paragraph (d)(1) of this section).

(2) Contacts with the FOIA Requester. See §806.27 for samples of language to use in various types of Air Force FOIA letters. If any part of a FOIA request is denied, and the requester appeals that denial, submit documents sent by Air Force elements to the requester in the FOIA appeal package in chronological order (see paragraph (d)(5) of this section). Letters that Air Force FOIA offices may need to send to a FOIA requester include:

(i) An initial notification letter that the FOIA request was received. This letter may advise the requester that processing of the FOIA request may be delayed because:

(A) All or part of the requested records are not located at the installation processing the FOIA request (see §806.29(c)(2)(ii)).

(B) An enormous number of records must be collected and reviewed.

(C) Other Air Force activities or other agencies, to include (if applicable) the nongovernment submitter of information, need to be involved in deciding whether or not to release the records.

(D) If you cannot complete processing of a FOIA request within 20 workdays, advise the requester of the reasons for the delay and give a date (within 30 workdays after receiving the request) when the requester can expect a final decision.

(ii) The initial notification letter may advise the requester all/part of the request was referred to another Air Force element or government activity.

(iii) The initial notification letter may advise the requester of the appropriate fee category. In cases where fees are appropriate, and requesters have not agreed to pay for responsive records and fees are likely to be more than \$15.00, seek assurances that the requester agrees to pay appropriate fees. If more information is needed to make a fee category determination, or to determine whether fees should be waived/reduced, inform the requester. FOIA offices may determine fee waiver/reduction requests before processing a FOIA request; if a fee waiver/reduction request is denied, the requester may

appeal that denial; he/she may also appeal an adverse fee category determination (e.g., asked for news media fees, but was assessed commercial fees.)

(iv) The initial notification letter may advise the requester the request does not sufficiently describe the desired records. If possible, help the requester identify the requested records by explaining what kind of information would make searching for responsive records easier.

(v) If Air Force elements can complete a FOIA request within the statutory 20-workday processing period, you may elect to send only a single letter to the requester, along with responsive records that are released to the requester in full.

(vi) A letter to the requester that the responding FOIA office uses multitrack processing due to a significant number of pending requests that prevents a response determination from being made within 20 workdays. This letter advises the FOIA requester that track the request is in (simple/complex); in this letter, if expedited processing was requested, the requester is advised if the request will be expedited or not. If the request is found to be complex, you must advise the requester he/she may alter the FOIA request to simplify processing. If it is determined the request will not be expedited, the requester must be told he/she can appeal. (This may be the initial letter to the requester, for Air Force elements with multitrack processing; if that is the case, this letter may include sections discussed in §806.29(c)(2)(i)).

(vii) Subsequent letters to the requester on various subjects (for example, releasing requested records; advising reasons for delays; responding to the letters, facsimiles or calls; advising the requester of referrals to other Air Force units or government activities; involves a non-Air Force submitter, etc.).

(viii) A release letter to the requester, forwarding releasable responsive records with a bill (if appropriate).

(ix) A “no records” response letter to the requester if there are no responsive records, or, a denial letter, if any responsive records are withheld from release. FOIA managers may sign “no

records” or “requested format not available” responses; they may also sign a letter that advises a requester the fee category sought was not determined to be appropriate, or that a fee waiver/fee reduction request was disapproved, or that a request for expedited processing has been denied. An IDA must sign any letter or document withholding responsive records. When denying records, you must tell the requester, in writing: the name and title or position of the official who made the denial determination, the basis for the denial in enough detail to permit the requester to make a decision concerning appeal, and the FOIA exemptions on which the denial is based. The denial letter must include a brief statement describing what the exemptions cover. When the initial denial is based (in whole or in part) on a security classification, this explanation should include a summary of the applicable executive order criteria for classification, as well as an explanation of how those criteria apply to the particular record in question. Estimate the volume of the records denied and provide this estimate to the requester, unless providing such an estimate would harm an interest protected by an exemption of the FOIA. This estimate should be in number of pages or, for records in other media, in some other reasonable form of estimation, unless the volume is otherwise indicated through deletions on records disclosed in part. Indicate the size and location of the redactions on the records released. You must also tell the requester how he/she can appeal the denial.

(3) Contacts with non-Air Force submitters of data. Before releasing data (information or records) submitted from outside the Air Force, determine whether you need to write to the submitter of the data for their views on releasability of their data. In many cases, this non-Air Force data may fall under FOIA Exemption 4. If it appears you must contact the submitter of the data, advise the requester in writing that you must give the submitter of the data the opportunity to comment before the Air Force decides whether to release the information. Give the submitter a reasonable period of time (30 calendar days) to object to release and

## § 806.29

## 32 CFR Ch. VII (7-1-12 Edition)

provide justification for withholding the documents. If the submitter does not respond, advise the submitter in writing that you have not received a reply and plan to release the records. Provide the submitter with the reasons the Air Force will release the records, and give the submitter your expected release date (at least 2 weeks from the date of your letter). This permits the submitter time to seek a temporary restraining order (TRO) in federal court, if they can convince the judge to issue such an order. See § 806.27 for samples of language to use in Air Force letters to both the FOIA requester and nongovernment submitters. Remember to include a copy of § 806.31 as an attachment to the letter sent to the nongovernment submitter.

(i) The notice requirements of this section need not be followed if the Air Force determines that the information should not be disclosed, the information has been lawfully published or officially made available to the public, or disclosure of the information is required by law.

(ii) If the submitter objects to release of the records, but the Air Force disclosure authority considers the records releasable, tell the submitter before releasing the data. Include in the letter to the submitter a brief explanation and a specific release date at least 2 weeks from the date of the letter. Advise the submitter once a determination is made that release of the data is required under the FOIA, failure to oppose the proposed release will lead to release of submitted data. Also advise the requester such a release under the FOIA will result in the released information entering the public domain, and that subsequent requests for the same information will be answered without any formal coordination between the Air Force and the submitter, unless the information is later amended, changed, or modified. A person equal to, or higher in rank than, the denial authority makes the final decision to disclose responsive records over the submitter's objection.

(iii) When a previously released contract document has been modified, any contract documents not in existence at the time of an earlier FOIA request that are responsive to a later FOIA re-

quest for the same contract, will be processed as a first-time FOIA request for those newly created documents. Notify the nongovernment submitter of the pending FOIA action, and give them the same opportunity to respond as is detailed above. Passage of a significant period of time since the prior FOIA release can also require Air Force elements to comply with the notice requirements in this paragraph.

(d) Denying all or part of a request. When responsive records are withheld from release (denied), the appropriate offices must prepare a denial package for the IDA. Air Force elements must send the request, related documents, and responsive records through their IDA's FOIA office to the IDA for a decision. The denial package must include:

(1) The FOIA request and any modifications by the requester.

(2) A copy of the responsive records, including both records that may be released and records recommended for denial.

(3) Written recommendations from the OPRs and an Air Force attorney.

(4) The exemptions cited and a discussion of how the records qualify for withholding under the FOIA. This discussion should also include the reasons for denial: to deny release of responsive records requested under the FOIA, you must determine that disclosure of the records would result in a foreseeable harm to an interest protected by a FOIA exemption (or exemptions), that the record is exempt from release under one or more of the exemptions of the FOIA, and that a discretionary release is not appropriate.

(5) Any collateral documents that relate to the requested records. For example:

(i) If the requested records came from a non-Air Force or non-U.S. Federal Government submitter, include any documents from the submitter that relate to the release or denial of the requested records. If you are not sure whether or not the non-Air Force or non-U.S. Federal Government submitted information is potentially exempt from release under the FOIA, contact an Air Force attorney. FOIA Exemptions 3, 4, 5, 6, and 7 may apply.

(ii) If the requested records came from Privacy Act systems of records,

## Department of the Air Force, DoD

## § 806.29

include a written discussion of any Privacy Act issues.

(iii) If any requested records came from another Air Force element, or release of the requested records would affect another Air Force element, FOIA offices should coordinate with that other element. If the FOIA request is not completely referred to the other element, include documents from that element.

(iv) If any requested records are classified, include a written certification from a classification authority or declassification authority stating the data was properly classified originally, that it remains properly classified (per E.O. 12958), and, if applicable, that no reasonably segregable portions can be released.

(e) FOIA appeal actions.

(1) If an IDA, or a FOIA office responding on behalf of an IDA, withholds a record from release because they determine the record is exempt under one or more of the exemptions to the FOIA, the requester may appeal that decision, in writing, to the Secretary of the Air Force. The appeal should be accompanied by a copy of the denial letter. FOIA appeals should be postmarked within 60 calendar days after the date of the denial letter, and should contain the reasons the requester disagrees with the initial denial. Late appeals may be rejected, either by the element initially processing the FOIA appeal, or by subsequent denial authorities, if the requester does not provide adequate justification for the delay. Appeal procedures also apply to the denial of a fee category claim by a requester, denial of a request for waiver or reduction of fees, disputes regarding fee estimates, review on an expedited basis of a determination not to grant expedited access to agency records, and for "no record" or "requested format not available" determinations when the requester considers such responses adverse in nature.

(2) Coordinate appeals with an Air Force attorney (and the OPR, if appropriate) so they can consider factual and legal arguments raised in the appeal, and can prepare written assessments of issues raised in the appeal to assist the IDA in considering the appeal.

MAJCOM FOIA offices and 11 CS/SCSR (for OPRs at HQ USAF and SAF), send all appeals to the Secretary of the Air Force through AFLSA/JACL for consideration, unless the IDA has reconsidered the initial denial action, and granted the appeal.

(3) If a requester appeals a "no records" determination, organizations must search again or verify the adequacy of their first search (for example, if a second search would be fruitless, the organization may include a signed statement from either the records OPR or the MAJCOM FOIA manager detailing why another search was not practical). The appeal package must include documents (to include a certification from the records OPR) that show how the organization tried to find responsive records. In the event a requester sues the Air Force to contest a determination that no responsive records exist, formal affidavits will be required to support the adequacy of any searches conducted.

(4) General administrative matters. FOIA requesters may ultimately sue the Air Force in federal court if they are dissatisfied with adverse determinations. In these suits, the contents of the administrative appeal file are evaluated to determine whether the Air Force complied with the FOIA and its own guidance. Improper or inadequate appeal files make defending these cases problematic. Include all the documents related to the requester's FOIA action in the appeal file. If appeal file documents are sensitive, or are classified up to the SECRET level, send them separately to AFLSA/JACL, 1501 Wilson Boulevard, 7th Floor, Arlington, VA 22209-2403. Make separate arrangements with AFLSA/JACL for processing classified appeal file documents TOP SECRET or higher. Cover letters on appeal packages need to list all attachments. If a FOIA action is complicated, a chronology of events helps reviewers understand what happened in the course of the request and appeal. If an appeal file does not include documentation described below, include a blank sheet in proper place and mark as "not applicable," "N/A," or "not used." Do not renumber and move the other items up. If any part of

## § 806.30

the requester's appeal is denied, the appeal package must include a signed statement by the IDA, demonstrating the IDA considered and rejected the requester's arguments, and the basis for that decision. This may be a separate memorandum, an endorsement on a legal opinion or OPR opinion, or the cover letter which forwards the appeal for final determination. Include in the cover letter forwarding the appeal to the Secretary of the Air Force the name, phone number and e-mail address (if any) of the person to contact about the appeal. The order and contents of appeal file attachments follow.

(i) The original appeal letter and envelope.

(ii) The initial FOIA request, any modifications of the request by the requester or any other communications from the requester, in chronological order.

(iii) The denial letter.

(iv) Copies of all records already released. (An index of released documents may be helpful, if there are a number of items. If the records released are "massive" (which means "several cubic feet") and AFLSA/JACL agrees, an index or description of the records may be provided in place of the released records. Do not send appeal files without copies of released records without the express agreement of AFLSA/JACL. Usually AFLSA/JACL requires all the released records in appeal files. If you do not send the released records to AFLSA/JACL when a FOIA requester has appealed a partial denial, retain a copy of what was released for 6 years.)

(v) Copies of all administrative processing documents, including extension letters, search descriptions, and initial OPR recommendations about the request, in chronological order.

(vi) Copies of the denied records or portions marked to show what was withheld. If your organization uses a single set of highlighted records (to show items redacted from records released to the requester), ensure the records are legible and insert a page in the appropriate place stating where the records are located. (An index of denied documents may be helpful, if there are a number of items. If the records denied are "massive" (which means

## 32 CFR Ch. VII (7-1-12 Edition)

"several cubic feet") and AFLSA/JACL agrees, an index or description of the records may be provided in place of the denied records. Do not send appeal files without copies of denied records without the express agreement of AFLSA/JACL. Usually AFLSA/JACL requires all the denied records in appeal files. If you do not send the denied records to AFLSA/JACL, when a FOIA requester has appealed a denial, retain a copy of what was denied for 6 years.)

(vii) All legal opinions in chronological order. Include a point-by-point discussion of factual and legal arguments in the requester's appeal (prepared by an Air Force attorney and/or the OPR). If the IDA does not state in the cover letter he/she signed, that he/she considered and rejected the requester's arguments, asserting the basis for that decision (e.g., the IDA concurs in the legal and/or OPR assessments of the requester's arguments) include a signed, written statement containing the same information from the IDA, either as a separate document or an endorsement to a legal or OPR assessment. Include any explanation of the decision-making process for intra-agency documents denied under the deliberative process privilege and how the denied material fits into that process (if applicable).

### § 806.30 FOIA exempt information examples.

(a) Certain responsive records may contain parts that are releasable, along with other parts that the Air Force must withhold from release. Carefully delete information exempt from release under the FOIA from copies of otherwise releasable records. Do not release copies that would permit the requester to "read through the marking." In order to assist FOIA managers in redacting records, selected items appropriate to withhold in commonly requested Air Force records are illustrated below. When providing releasable portions from classified paragraphs, line through and do not delete, the classification marking preceding the paragraph.

(b) Exemption 1. Example used is an extract from a "simulated" contingency plan (all information below is

**Department of the Air Force, DoD**

**§ 806.30**

fictional and UNCLASSIFIED; parenthetical information and marking is used for illustrative purposes only).

(U) Air Force members will safeguard all FELLOW YELLOW data (NOTE: FELLOW YELLOW simulates an UNCLASSIFIED code name).

During the contingency deployment in Shambala, those members assigned to force element FELLOW YELLOW will cover their movements by employing specified camouflage and concealment activities while behind enemy lines. Only secure communications of limited duration as specified in the communications annex will be employed until FELLOW YELLOW personnel return to base. (Exemption 1)

(c) Exemption 2. Example used is an extract from a “simulated” test administration guide (all information below is fictional and is used for illustrative purposes only).

When administering the test to determine which technicians are ranked fully qualified, make sure to allow only the time specified in HQ AETC Pamphlet XYZ, which the technicians were permitted to review as part of their test preparation. For ease in scoring this exam, correct answers are A, A, B, B, A, B, C, C, A, B, D, D, C, C, C, D; the corresponding template for marking the standard answer sheet is kept locked up at all times when not in use to grade answer sheets. (Exemption “high” 2)

(d) Exemption 5. Example used is a simulated IG Report of Investigation (ROI) recommendation. All parenthetical information in this example is fictional and is used for illustrative purposes only:

Having interviewed the appropriate personnel and having reviewed the appropriate documents, I recommend additional training sessions for all branch personnel on accepted Air Force standards, and the Air Force pursue administrative or judicial disciplinary action with respect to Terry Hardcase. (Exemption 5)

(e) Exemption 6. Example used is a simulated personnel computer report on a military member selected for a special assignment (all information below is fictional; information and marking is used for illustrative purposes only.):

SSgt Doe, Kerry E.	SSN: 111-11-1112	Date of Birth: 22 Jun 71
Duty Title: Special Assistant to CINCPAC	Office Symbol: CINCPAC/CCSA	

Duty Station: Hickam AFB HI 11111-1111	Date Assigned: 12 June 1998	
Marital Status: Divorced	Dependents: 01	Home Address: 12 Anystreet, Downtown ST 11112
Home Phone: (112) 223-3344 (Exemption 6)		

(f) Exemption 7. Example used is summary of a law enforcement report on a domestic disturbance at on-base family housing (all information below is fictional and all parenthetical information is used for illustrative purposes only):

At 2140, the law enforcement desk, extension 222-3456, took an anonymous call that reported a disturbance at 1234 Basestreet, quarters allegedly occupied by two military members. SrA Patrolman (names of law enforcement investigators usually are withheld under Exemptions 6 and 7(C)) arrived on the scene at 2155. SrA Patrolman met Nora Neighbor, (names of witnesses usually are withheld under Exemptions 6 and 7(C)) who was very agitated. Because she feared her neighbors would retaliate against her if they knew she reported their fight, she asked that her name not be released before she would talk. After she was promised her identity would remain anonymous, she stated: (Nora Neighbor became a confidential informant; data that could identify her, and in some cases, the information she related, should be withheld from release under Exemptions 6, 7(C) and (D).) “I heard cursing and heard furniture and dishes breaking. They fight all the time. I’ve seen Betty Battle (unless Betty is the requester, redact her name Exemptions 6 and 7(C)) with a black eye, and I also saw Bob Battle (unless Bob is the requester, redact his name Exemptions 6 and 7(C)) with bruises the day after they had their last fight, last Saturday night. This time, there was a tremendous crash; I heard a man scream “My Lord NO!” then I saw Betty Battle come out of the house with dark stains on her clothes—she got into her car and drove away. I could see this really well, because the streetlight is right between our houses; I’m the wife of their NCOIC. If only Nick, my husband, was here now, he’d know what to do! I haven’t heard anything from Bob Battle.” (Exemptions 6 and 7)

**§ 806.31 Requirements of 5 U.S.C. 552(b)(4) to submitters of non-government contract-related information.**

(a) The FOIA requires federal agencies to provide their records, except those specifically exempted, for the public to inspect and copy. Section (b) of the Act lists nine exemptions that are the only basis for withholding records from the public.

(b) In this case, the fourth exemption, 5 U.S.C. 552(b)(4), may apply to records or information the Air Force maintains. Under this exemption, agencies must withhold trade secrets and commercial or financial information they obtained from a person or organization outside the government that is privileged or confidential. This generally includes information provided and received during the contracting process with the understanding that the Air Force will keep it privileged or confidential.

(c) Commercial or financial matter is “confidential” and exempt if its release will probably:

(1) Impair the government’s ability to obtain necessary information in the future.

(2) Substantially harm the source’s competitive position or impair some other legitimate government interest such as compliance and program effectiveness.

(d) Applicability of exemption. The exemption may be used to protect information provided by a nongovernment submitter when public disclosure will probably cause substantial harm to its competitive position. Examples of information that may qualify for this exemption include:

(1) Commercial or financial information received in confidence with loans, bids, contracts, or proposals, as well as other information received in confidence or privileged, such as trade secrets, inventions, discoveries, or other proprietary data.

NOTE: Certain proprietary and source selection information may also fall under exemption (b)(3), under the provisions of 10 U.S.C. 2305(g) or 41 U.S.C. 423, if statutory requirements are met.

(2) Statistical data and commercial or financial information concerning contract performance, income, profits,

losses, and expenditures, offered and received in confidence from a contractor or potential contractor.

(3) Personal statements given during inspections, investigations, or audits, received and kept in confidence because they reveal trade secrets or commercial or financial information, normally considered confidential or privileged.

(4) Financial data that private employers give in confidence for local wage surveys used to set and adjust pay schedules for the prevailing wage rate of DoD employees.

(5) Information about scientific and manufacturing processes or developments that is technical or scientific or other information submitted with a research grant application, or with a report while research is in progress.

(6) Technical or scientific data a contractor or subcontractor develops entirely at private expense, and technical or scientific data developed partly with Federal funds and partly with private funds, in which the contractor or subcontractor retains legitimate proprietary interests per 10 U.S.C. 2320 to 2321 and 48 CFR, Chapter 2, 227.71-227.72.

(7) Computer software copyrighted under the Copyright Act of 1976 (17 U.S.C. 106), the disclosure of which would adversely impact its potential market value.

(e) Submitter’s Written Response. If release of the requested material would prejudice your commercial interests, give detailed written reasons that identify the specific information and the competitive harm public release will cause to you, your organization, or your business. The act requires the Air Force to provide any reasonably segregable part of a record after deleting exempt portions. If deleting key words or phrases would adequately protect your interests, advise us in writing which portions you believe we can safely release, and which portions you believe we need to withhold from release. If you do not provide details on the probability of substantial harm to your competitive position or other commercial interests, which would be caused by releasing your material to the requester, we may be required to release the information. Records qualify for protection on a case by case basis.

(f) Pricing Information. Generally, the prices a contractor charges the government for goods or services would be released under the FOIA. Examples of releasable data include: bids submitted in response to an invitation for bids (IFB), amounts actually paid by the government under a contract, and line item prices, contract award price, and modifications to a contract. Unit prices contained in a contract award are considered releasable as part of the post award notification procedure prescribed by 48 CFR 15.503, unless they are part of an unsuccessful proposal, then 10 U.S.C. 2305(g) protects everything including unit price.

APPENDIX A TO PART 806—REFERENCES

Title 5, United States Code, Section 552, The Freedom of Information Act, as amended  
 Title 5, United States Code, Section 552a, The Privacy Act (as amended)  
 Title 10, United States Code, Section 2305(g), Prohibition on Release of Contractor Proposals  
 Title 48, Code of Federal Regulations (CFR), Federal Acquisition Regulations (FAR) System  
 OMB Bulletin 95-01, 7 December 1994  
 OMB Memorandum, 6 February 1998  
 DoD 5200.1-R, Information Security Program, January 1997  
 AFI 16-701, Special Access Programs  
 AFI 31-206, Security Police Investigations  
 AFI 31-401, Information Security Program Management  
 AFI 31-501, Personnel Security Program Management  
 AFI 31-601, Industrial Security Program Management  
 AFI 33-129, Transmission of Information Via the Internet  
 AFI 35-205, Air Force Security and Policy Review Program  
 AFI 36-2603, Air Force Board for Correction of Military Records  
 AFI 36-2706, Military Equal Opportunity and Treatment Program  
 AFI 36-2906, Personal Financial Responsibility  
 AFI 36-2907, Unfavorable Information File (UIF) Program  
 AFPD 37-1, Air Force Information Management (will convert to AFPD 33-3)  
 AFI 37-124, The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections (will convert to AFI 33-324)  
 AFI 37-132, Air Force Privacy Act Program (will convert to AFI 33-332)  
 AFMAN 37-139, Records Disposition Schedule (will convert to AFMAN 33-339)

AFI 40-301, Family Advocacy  
 AFI 41-210, Patient Administration Functions  
 AFI 44-109, Mental Health and Military Law  
 AFI 51-201, Administration of Military Justice  
 AFI 51-301, Civil Litigation  
 AFI 51-303, Intellectual Property-Patents, Patent Related Matters, Trademarks, and Copyrights  
 AFI 51-501, Tort Claims  
 AFI 51-503, Aircraft, Missile, Nuclear and Space Accident Investigations  
 AFI 51-504, Legal Assistance, Notary and Preventive Law Programs  
 AFI 51-1102, Cooperation with the Office of the Special Counsel  
 AFI 61-204, Disseminating Scientific and Technical Information  
 AFI 61-303, Licensing Inventions Made Under Cooperative Research and Development Agreements  
 AFI 65-401, Relations With the General Accounting Office  
 AFI 71-101, Volume 1, Criminal Investigations  
 AFI 71-101, Volume 2, Protective Service Matters  
 AFI 84-101, Historical Products, Services, and Requirements  
 AFI 90-301, Inspector General Complaints  
 AFI 90-401, Air Force Relations With Congress  
 AFI 91-204, Safety Investigations and Reports

APPENDIX B TO PART 806—  
 ABBREVIATIONS AND ACRONYMS

AFCA—Air Force Communications Agency  
 AFCIC—Air Force Communications and Information Center  
 AFRC—Air Force Reserve Command  
 AFI—Air Force Instruction  
 AFLSA/JACL—Air Force Legal Services Agency, General Litigation Division  
 AFMAN—Air Force Manual  
 AFPC/MSIMD—Air Force Personnel Center/Records Management, FOIA, and Privacy Act Office  
 AFPD—Air Force Policy Directive  
 ANG—Air National Guard  
 ASCII—American Standard Code for Information Interchange  
 CFR—Code of Federal Regulations  
 DFAS—Defense Finance and Accounting Service  
 DFOISR—Director, Freedom of Information and Security Review  
 DoD—Department of Defense  
 DRU—Direct Reporting Unit  
 EFOIA—Electronic Freedom of Information Act  
 ERR—Electronic Reading Room  
 FOA—Field Operating Agency  
 FOIA—Freedom of Information Act  
 FOUO—For Official Use Only

**Pt. 806, App. C**

GAO—General Accounting Office  
GILS—Government Information Locator Service  
GPO—Government Printing Office  
IDA—Initial Denial Authority  
IG—Inspector General  
IMPAC—International Merchant Purchase Authority Card  
LOA—Letters of Offer and Acceptance  
MAJCOM—Major Command  
MFR—Memorandum for Record  
NATO—North Atlantic Treaty Organization  
NORAD—North American Aerospace Defense  
NTIS—National Technical Information Service  
OCR—Office of Corollary Responsibility  
OMB—Office of Management and Budget  
OPR—Office of Primary Responsibility  
PA—Privacy Act  
PAO—Public Affairs Office  
PAS—Personnel Accounting Symbol  
RCS—Reports Control Symbol  
SAF—Secretary of the Air Force  
SSN—Social Security Number  
USAF—United States Air Force  
U.S.C.—United States Code  
WWW—World Wide Web

**APPENDIX C TO PART 806—TERMS**

Appellate Authority—The Office of the General Counsel to the Secretary of the Air Force (SAF/GCA).  
Denial—An adverse determination on no records, fees, expedited access, or not disclosing records.  
Determination—The written decision to release or deny records or information that is responsive to a request.  
Disclosure—Providing access to, or one copy of, a record.  
Disclosure Authority—Official authorized to release records, normally division chiefs or higher.  
FOIA Manager—The person who manages the FOIA Program at each organizational level.  
FOIA Request—A written request for DoD records from the public that cites or implies the FOIA.  
Functional Request—Any request for records from the public that does not cite the FOIA.  
Government Information Locator Service (GILS)—An automated on-line card catalog of publicly accessible information.  
Glomar Response—A reply that neither confirms nor denies the existence or nonexistence of the requested record.  
Initial Denial Authority (IDA)—Persons in authorized positions that may withhold records.  
Partial Denial—A decision to withhold part of a requested record.  
Public Interest—The interest in obtaining official information that sheds light on how an agency performs its statutory du-

**32 CFR Ch. VII (7–1–12 Edition)**

ties and informs citizens about what their government is doing.  
Reading Room—A place where the public may inspect and copy, or have copied, releasable records.  
Records—The products of data compilation, such as all books, papers, maps, and photographs, machine readable materials inclusive of those in electronic form or format, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the U.S. Government under Federal Law in connection with the transaction of public business and in the agency's possession and control at the time the FOIA request is made. Records include notes, working papers, and drafts.  
Redact—To remove nonreleasable material.

**PART 806<sup>b</sup>—PRIVACY ACT PROGRAM**

**Subpart A—Overview of the Privacy Act Program**

Sec.  
806b.1 Summary of revisions.  
806b.2 Basic guidelines.  
806b.3 Violation penalties.  
806b.4 Privacy Act complaints.  
806b.5 Personal notes.  
806b.6 Systems of records operated by a contractor.  
806b.7 Responsibilities.

**Subpart B—Obtaining Law Enforcement Records and Confidentiality Promises**

806b.8 Obtaining law enforcement records.  
806b.9 Confidentiality promises.

**Subpart C—Collecting Personal Information**

806b.10 How to collect personal information.  
806b.11 When To Give Privacy Act Statements (PAS).  
806b.12 Requesting the Social Security Number.

**Subpart D—Giving Access to Privacy Act Records**

806b.13 Making a request for access.  
806b.14 Processing a request for access.  
806b.15 Fees.  
806b.16 Denying or limiting access.  
806b.17 Special provision for certain medical records.  
806b.18 Third party information in a Privacy Act System of records.  
806b.19 Information compiled in anticipation of civil action.  
806b.20 Denial authorities.

## Department of the Air Force, DoD

## § 806b.2

### Subpart E—Amending the Record

- 806b.21 Amendment reasons.
- 806b.22 Responding to amendment requests.
- 806b.23 Approving or denying a record amendment.
- 806b.24 Seeking review of unfavorable Agency determinations.
- 806b.25 Contents of Privacy Act case files.

### Subpart F—Appeals

- 806b.26 Appeal procedures.

### Subpart G—Privacy Act Notifications

- 806b.27 When to include a Privacy Act warning statement in publications.
- 806b.28 Warning banners.
- 806b.29 Sending personal information over electronic mail.

### Subpart H—Privacy Impact Assessments

- 806b.30 Evaluating information systems for Privacy Act compliance.

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

- 806b.31 Publishing System notices.
- 806b.32 Submitting notices for publication in the FEDERAL REGISTER.
- 806b.33 Reviewing notices.

### Subpart J—Protecting and Disposing of Records

- 806b.34 Protecting records.
- 806b.35 Balancing protection.
- 806b.36 Disposing of records.

### Subpart K—Privacy Act Exemptions

- 806b.37 Exemption types.
- 806b.38 Authorizing exemptions.
- 806b.39 Requesting an exemption.
- 806b.40 Exemptions.

### Subpart L—Disclosing Records to Third Parties

- 806b.41 Disclosure considerations.
- 806b.42 Social rosters.
- 806b.43 Placing personal information on shared drives.
- 806b.44 Personal information that requires protection.
- 806b.45 Releasable information.
- 806b.46 Disclosing other information.
- 806b.47 Rules for releasing Privacy Act information without the consent of the subject.
- 806b.48 Disclosing the medical records of minors.
- 806b.49 Disclosure accountings.
- 806b.50 Computer matching.
- 806b.51 Privacy and the Web.

### Subpart M—Training

- 806b.52 Who needs training?
- 806b.53 Training tools.
- 806b.54 Information collections, records, and forms or Information Management Tools (IMT).

APPENDIX A TO PART 806b—DEFINITIONS

APPENDIX B TO PART 806b—PREPARING A SYSTEM NOTICE

APPENDIX C TO PART 806b—DoD “BLANKET ROUTINE USES”

APPENDIX D TO PART 806b—GENERAL AND SPECIFIC EXEMPTIONS

APPENDIX E TO PART 806b—PRIVACY IMPACT ASSESSMENT

AUTHORITY: Pub. L. 93-579, 88 Stat. 1896 (5 U.S.C. 552a).

SOURCE: 69 FR 954, Jan. 7, 2004, unless otherwise noted.

## Subpart A—Overview of the Privacy Act Program

### § 806b.1 Summary of revisions.

This part moves responsibility for the Air Force Privacy Program from Air Force Communications and Information Center to the Air Force Chief Information Officer; prescribes Air Force Visual Aid 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 Air Force Communications and Information Center to Air Force Legal Services Agency; 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*<sup>1</sup> and applies to records on living U.S. citizens and permanent resident aliens that are retrieved by name or

<sup>1</sup> <http://www.usdoj.gov/04foia/privstat.htm>.

### § 806b.3

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 requirements and are referred to as Privacy Act 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 B 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, and is within the scope of, an authorized law enforcement activity. First Amendment rights include, but are not limited to, freedom of religion, freedom of political beliefs, freedom of speech, freedom of the press, the right to assemble, and the right to petition.

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

(d) Air Force members will:

(1) Keep paper and electronic records that are retrieved by name or personal identifier only in approved Privacy Act 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.

### 32 CFR Ch. VII (7-1-12 Edition)

(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 (5 U.S.C. 552a(d)(5)).

(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 Privacy Act. 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.

(a) Process Privacy Act complaints or allegations of Privacy Act violations through the appropriate base or Major Command Privacy Act office, to the local systems manager. The base or Major Command Privacy Act officer directs the process and provides guidance to the system manager. The local systems manager will investigate complaints, or allegations of Privacy Act 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 Privacy Act Officer. In cases where no system manager can be identified, the local Privacy Act officer will assume these duties. Issues that cannot be resolved at the local level will be elevated to the Major Command 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 Staff Judge Advocate. In combatant commands, process component unique system complaints through the respective component chain of command.

(b) For Privacy Act complaints filed in a U.S. District Court against the Air Force, an Air Force activity, or any Air Force employee, Air Force Legal Services Agency, General Litigation Division (JACL) will provide Air Force Chief Information Officer/P a litigation summary to include: The case number, requester name, the nature of the case (denial of access, refusal to amend, incorrect records, or specify the particular violation of the Privacy Act), date complaint filed, court, defendants, and any appropriate remarks, as well as updates during the litigation process. When the court renders a formal opinion or judgment, Air Force Legal Services Agency, General Litigation Division (JACL) sends Air Force Chief Information Officer/P a copy of the judgment and opinion.

#### § 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: Keeping or destroying the records is not at the sole discretion of the author; the notes are required by oral or written directive, regulation, or command policy; or 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 Privacy Act 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 Privacy Act 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 Major Command 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 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, Fiscal and Administrative Law Division (GCA) makes final decisions on appeals.

(c) The General Litigation Division, Air Force Legal Services Agency (JACL), receives Privacy Act appeals and provides recommendations to the appellate authority. Service unique appeals, from combatant commands, should go through the respective chain of command.

(d) The Plans and Policy Directorate, Office of the Chief Information Officer manages the program through the Air Force Privacy Act 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 Major Commands, field operating agencies, direct reporting units and combatant commands for which AF is executive agent in their implementation and execution of the Air Force Privacy Program. Ensures availability of training and training tools for a variety of audiences.

**§ 806b.8**

**32 CFR Ch. VII (7–1–12 Edition)**

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

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

(f) 11th Communications Squadron will provide Privacy Act training and submit Privacy Act reports for Headquarters United States Air Force and Secretary of the Air Force offices.

(g) Major Command Commanders: Appoint a command Privacy Act officer, and send the name, office symbol, phone number, and e-mail address to Air Force Chief Information Officer/P.

(h) Major Command and Headquarters Air Force Functional Chief Information Officers:

(1) Review and provide final approval on Privacy Impact Assessments (*see* appendix E of this part).

(2) Send a copy of approved Privacy Impact Assessments to Air Force Chief Information Officer/P.

(i) Major Command Privacy Act Officers:

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

(2) Promote Privacy Act awareness throughout the organization.

(3) Review publications and forms for compliance with this part (do forms require a Privacy Act Statement; is Privacy Act Statement 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 for information systems.

(8) Resolve complaints or allegations of Privacy Act violations.

(9) Review and process denial recommendations.

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

(j) Base Privacy Act 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 Privacy Act requirements.

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

(4) Prepare system notices and reports.

(5) Answer Privacy Act requests.

(6) Records of disclosures.

(7) Validate system notices annually.

(8) Investigate Privacy Act complaints.

(1) System owners and developers:

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

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

(3) Complete a Privacy Impact Assessment and submit to the Privacy Act Officer.

**Subpart B—Obtaining Law Enforcement Records and Confidentiality Promises**

**§ 806b.8 Obtaining law enforcement records.**

The Commander, Air Force Office of Special Investigation; the Commander, Air Force Security Forces Center; Major Command, Field Operating Agency, and base chiefs of security forces; Air Force Office of Special Investigations 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).**

(a) 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 Privacy Act Statement if asked. Do not ask the person to sign the Privacy Act Statement.

(b) A Privacy Act Statement 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 non-threatening language.

**§ 806b.12 Requesting the Social Security Number.**

When asking an individual for his or her Social Security Number, always give a Privacy Act Statement that tells the person: The legal authority for requesting it; the uses that will be made of the Social Security Number; and whether providing the Social Security Number is voluntary or mandatory. Do not deny anyone a legal right, benefit, or privilege for refusing to give their Social Security Number unless the law requires disclosure, or a law or regulation adopted before January 1, 1975 required the Social Security Number 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 Social Security Number 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 Social Security Number as a service or employment number to reference the individual’s official records. When you ask someone for a Social Security Number 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*<sup>2</sup>, authorizes using the Social Security Number as a personal identifier. This order is not adequate authority to collect a Social Security Number to create a record. When law does not require disclosing the Social Security Number or when the system of records was created after January 1, 1975, you may ask for the Social Security Number, but the individual does not have to disclose it. If the individual refuses to respond, use alternative means of identifying records. (c) Social Security Numbers 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.

<sup>2</sup>[http://resource.lawlinks.com/content/legal\\_research/Executive\\_Orders/1940-1960/executive\\_order\\_9397.htm](http://resource.lawlinks.com/content/legal_research/Executive_Orders/1940-1960/executive_order_9397.htm).

## § 806b.13

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 and the Privacy Act 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.defenseink.mil/privacy/notices/usaf>.

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

## 32 CFR Ch. VII (7–1–12 Edition)

(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 D 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 Privacy Act, provide any parts releasable under the Freedom of Information Act, with appeal rights (See subpart F of this part), citing appropriate exemptions from the Privacy Act and the Freedom of Information Act, 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.

Fee waivers. Waive fees automatically if the direct cost of reproduction is less than \$15, unless the individual is seeking an obvious extension or duplication of a previous request for which he or she was granted a waiver. Decisions to waive or reduce fees that exceed \$15 are made on a case-by-case basis.

**§ 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 Privacy Act office. Judge Advocate offices will include a written legal opinion. The Privacy Act 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 rule published in the FEDERAL REGISTER as a final rule.
- (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.
- (c) 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 sub-

ject's records). Consult your servicing Staff Judge Advocate 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 Air Force Chief Information Officer/P with the position titles of designees. Authorities are:

- (a) Deputy Chief of Staffs and chiefs of comparable offices or higher level at Secretary of the Air Force or Headquarters United States Air Force or designees.
- (b) Major Command, Field Operating Agency, or direct reporting unit commanders or designees.
- (c) Director, Personnel Force Management, 1040 Air Force Pentagon, Washington, DC 20330-1040 (for civilian personnel records).
- (d) Commander, Air Force Office of Special Investigations, Washington, DC 20332-6001 (for Air Force Office of Special Investigations 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

### § 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 Privacy Act office. Legal offices will include a written legal opinion. The Privacy Act 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. Record correction requests denied by the Air Force Board for Correction of Military Records are not subject to further consideration under this part. Military personnel, other than

## 32 CFR Ch. VII (7-1-12 Edition)

U.S. Air Force personnel, should pursue service-unique record corrections through their component chain of command.

### § 806b.25 Contents of Privacy Act 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 Air Force Legal Services Agency, General Litigation Division (JACL). The package must include:

(1) The original appeal letter;

(2) The initial request;

(3) The initial denial;

(4) A copy of the record;

(5) Any internal records or coordination actions relating to the denial;

(6) The denial authority's comments on the appellant's arguments; and

(7) The legal reviews.

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

(b) Air Force Legal Services Agency, General Litigation Division (JACL) reviews the denial and provides a final recommendation to Secretary of the Air Force, Fiscal and Administrative Law Division (GCA). Secretary of the

## Department of the Air Force, DoD

## § 806b.29

Air Force, Fiscal and Administrative Law Division (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 Secretary of the Air Force, Fiscal and Administrative Law Division (GCA) denies the request to amend the record. Secretary of the Air Force, Fiscal and Administrative Law Division (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 Secretary of the Air Force, Fiscal and Administrative Law Division (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 Privacy Act 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 Social Security Number, or any part of the Social Security Number, from the individual. The warning statement will cite legal authority and when part of a record system, the Privacy Act 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 Privacy Act 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 Air Force Instruction 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 Air Force Instruction 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/Air Force Supp,

## § 806b.30

Chapter 4<sup>3</sup>, provides additional guidance regarding For Official Use Only 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 Privacy Act 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 Privacy Act 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.

(a) The Privacy Impact Assessment 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 the individual to decline or consent to providing 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<sup>4</sup> requires Privacy Impact Assessments to be conducted before:

(1) Developing or procuring information technology systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public.

<sup>3</sup> [http://www.dtic.mil/whs/directives/corres/pdf/54007r\\_0998/p54007r.pdf](http://www.dtic.mil/whs/directives/corres/pdf/54007r_0998/p54007r.pdf).

<sup>4</sup> [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107\\_cong\\_public\\_laws&docid=f:publ347.107.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf).

## 32 CFR Ch. VII (7–1–12 Edition)

(2) Initiating a new electronic collection of information in identifiable form for 10 or more persons excluding agencies, instrumentalities, or employees of the Federal Government.

(b) In general, Privacy Impact Assessments are required to be performed and updated as necessary where a system change creates new privacy risks.

(c) No Privacy Impact Assessment is required where information relates to internal government operations, has been previously assessed under an evaluation similar to a Privacy Impact Assessment, or where privacy issues are unchanged.

(d) The depth and content of the Privacy Impact Assessment should be appropriate for the nature of the information to be collected and the size and complexity of the information technology system.

(e) The system owner will conduct a Privacy Impact Assessment as outlined in appendix E to this part and send it to their Major Command Privacy Act office for review and final approval by the Major Command or Headquarters Air Force Functional Chief Information Officer. The Major Command or Headquarters Air Force Functional Chief Information Officer will send a copy of approved Privacy Impact Assessments to Air Force Chief Information Officer/P, 1155 Air Force Pentagon, Washington DC 20330-1155; or e-mail [af.foia@pentagon.af.mil](mailto:af.foia@pentagon.af.mil).

(f) Whenever practicable, approved Privacy Impact Assessments will be posted to the Freedom of Information Act/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).

### 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

## Department of the Air Force, DoD

## § 806b.36

is implemented or changed. The Privacy Act also requires submission of new or significantly changed systems to the Office of Management and Budget 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 Major Command Privacy Office, to Air Force Chief Information Officer/P. Send notices electronically to [af.foia@pentagon.af.mil](mailto: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 B to this part. For new systems, system managers must include a statement that a risk assessment was accomplished and is available should the Office of Management and Budget request it.

### § 806b.33 Reviewing notices.

System managers will review and validate their Privacy Act system notices annually and submit changes to Air Force Chief Information Officer/P through the Major Command 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/Air Force 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 Air Force Instruction 33-202, *Computer Security*,<sup>5</sup> for procedures on safeguarding personal information in automated records.

(a) AF Form 3227, Privacy Act Cover Sheet,<sup>6</sup> 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/Air Force Supp.

(b) Privacy Act Labels. Use of Air Force Visual Aid 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.

<sup>5</sup> <http://www.e-publishing.af.mil/pubfiles/af/33/afi33-202/afi33-202.pdf>.

<sup>6</sup> <http://www.e-publishing.af.mil/formfiles/af/af3227/af3227.xfd>.

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 Privacy Act 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 Privacy Act.

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

#### § 806b.38 Authorizing exemptions.

Denial authorities may withhold records using Privacy Act exemptions only when an exemption for the system of records has been published in the FEDERAL REGISTER as a final rule. Appendix D lists the systems of records that have published 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 Privacy Act will send a request to Air Force Chief Information Officer/P through the Major Command or Field Operating Agency Privacy Act 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 Privacy Act from which the system is to be exempted, with justification for each subsection.

#### § 806b.40 Exemptions.

Exemptions permissible under 5 U.S.C. 552a (subject to §806b.38 of this part):

(a) *The (j)(2) exemption*. Applies to investigative records created and main-

tained by law-enforcement activities whose principal function is criminal law enforcement.

(b) *The (k)(1) exemption*. Applies to information specifically authorized to be classified under the DoD Information Security Program Regulation, 32 CFR part 159.

(c) *The (k)(2) exemption*. Applies to investigatory information compiled for law-enforcement purposes by nonlaw enforcement activities and which is not within the scope of Sec. 806b.40(a) of this part. 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).

(d) *The (k)(3) exemption*. Applies to records maintained in connection with providing protective services to the President and other individuals under 18 U.S.C. 3506.

(e) *The (k)(4) exemption*. Applies to records maintained solely for statistical research or program evaluation purposes and which are not used to make decisions on the rights, benefits, or entitlement of an individual except for census records which may be disclosed under 13 U.S.C. 8.

(f) *The (k)(5) exemption*. Applies to 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, but only to the extent such material would reveal the identity of a confidential source. This provision allows protection of confidential sources used in background investigations, employment inquiries, and similar inquiries that are for personnel screening to determine suitability, eligibility, or qualifications.

(g) *The (k)(6) exemption*. Applies to testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal or military service, if the disclosure would compromise the objectivity or fairness of the test or examination process.

(h) *The (k)(7) exemption.* Applies to evaluation material used to determine potential for promotion in the Military Services, but only to the extent that the disclosure of such material would reveal the identity of a confidential source.

### 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 Privacy Act applies (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 Postal Service Center Directory<sup>7</sup>(see Air Force Instruction 33-329, *Base and Unit Personnel Locators*<sup>8</sup>).

#### § 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.

<sup>7</sup> <http://www.e-publishing.af.mil/formfiles/af/af624/af624.xfd>

<sup>8</sup> <http://www.e-publishing.af.mil/pubfiles/af/33/afi33-329/afi33-329.pdf>.

#### § 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

**§ 806b.46**

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 (Continental United States (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

**32 CFR Ch. VII (7-1-12 Edition)**

than the subject of the record without his or her 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 official duties.
- (b) *Exception 2.* In response to a Freedom of Information Act request for information contained in a system of records about an individual and the Freedom of Information Act requires release of the information.
- (c) *Exception 3.* To agencies outside DoD only for a Routine Use published in the FEDERAL REGISTER. The purpose of the disclosure must be compatible with the intended purpose of collecting and maintaining the record. When initially collecting the information from the subject, the Routine Uses block in the Privacy Act Statement must name the agencies and reason.

NOTE TO PARAGRAPH (C): In addition to the Routine Uses established by the Department of the Air Force within each system of records, the DoD has established "Blanket Routine Uses" that apply to all record systems maintained by the Department of the Air Force. These "Blanket Routine Uses" have been published only once at the beginning of the Department of the Air Force's FEDERAL REGISTER compilation of record systems notices in the interest of simplicity, economy and to avoid redundancy. Unless a system notice specifically excludes a system of records from a "Blanket Routine Use," all "Blanket Routine Uses" apply to that system (see appendix C to this part).

- (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 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. In addition, the “blanket routine use” for law enforcement allows the system manager to disclose a record to a law enforcement agency if the agency suspects a criminal violation.

(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 Air Force Instruction 90-401, Air Force Relations With Congress).<sup>9</sup>

(1) 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.

(2) Requests from a Congressional member not on behalf of a committee or the record subject are properly analyzed under the Freedom of Information Act, and not under the Privacy Act.

(j) *Exception 10.* The Comptroller General or an authorized representative of the General Accounting Office (GAO) to conduct official GAO business.

(k) *Exception 11.* A court of competent jurisdiction, with a court order signed by a judge.

(l) *Exception 12.* A consumer reporting agency in accordance with 31 U.S.C. 3711(e). Ensure category element is represented within the system of records notice.

#### § 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 guide-

lines. 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 Staff Judge Advocate.

(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 Freedom of Information Act. System managers may use Air Force Form 771<sup>10</sup>, 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

<sup>9</sup> <http://www.e-publishing.af.mil/pubfiles/af/90/afi90-401/afi90-401.pdf>.

<sup>10</sup> <http://www.e-publishing.af.mil/formfiles/af/af771/af771.xfd>.

## § 806b.51

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 Privacy Act:

- (1) Prepare a written agreement between participants;
- (2) Secure approval of the Defense Data Integrity Board;
- (3) Publish a matching notice in the FEDERAL REGISTER before matching begins;
- (4) Ensure full investigation and due process; and
- (5) Act on the information, as necessary.

(a) The Privacy Act 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 Privacy Act matching requirements.

(c) Any activity that expects to participate in a matching program must contact Air Force Chief Information Officer/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 Air Force Chief Information Officer/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 Air Force Chief Information Officer/P through the Major Command Privacy Act Officer.

## 32 CFR Ch. VII (7-1-12 Edition)

### § 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 Air Force Instruction 33-129 *Transmission of Information Via the Internet*.<sup>11</sup>

(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 is voluntary, and notify users 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.*, Social Security Number). We may only maintain such information in approved Privacy Act 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 Privacy Act 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—

<sup>11</sup> <http://www.e-publishing.af.mil/pubfiles/af/33/afi33-129/afi33-129.pdf>.

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 Freedom of Information Act Web page which includes a Privacy Overview, Privacy Act 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 Major Command and base Privacy Act officers, available from the Freedom of Information Act 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 Air Force Chief Information Officer/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 Privacy Act records according to Air Force Manual 37-139, Records Disposition Schedule.<sup>12</sup>

(c) Forms or Information Management Tools (Adopted and Prescribed).

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

(2) Prescribed Forms or Information Management Tools. AF Form 3227, Privacy Act Cover Sheet, Air Force Form 771, Accounting of Disclosures, and Air Force Visual Aid 33-276.

#### APPENDIX A TO PART 806b—DEFINITIONS

*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.

<sup>12</sup> <http://www.e-publishing.af.mil/pubfiles/af/37/afman37-139/afman37-139.pdf>.

*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 Social Security Number.

*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 B TO PART 806b—PREPARING A SYSTEM NOTICE

The following elements comprise a system of records notice for publication in the FEDERAL REGISTER:

*System identifier:* Air Force Chief Information Officer/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 Deputy Chief of Staff. 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 Social Security Number as a personal identifier. Include this authority whenever the Social Security Number 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:* List each specific agency or activity outside DoD to whom the records may be released and the purpose for such release.

The DoD 'Blanket Routine Uses' published in the Air Force Directory of System Notices

apply to all system notices unless you indicate otherwise.

*Policies 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, Social Security Number, 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 Air Force Manual 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, Social Security Number, 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:* Air Force Chief Information Officer/P provides this standard caption.

*Record source categories:* Show categories of individuals or other information sources for the system.

*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 C TO PART 806b—DoD 'BLANKET ROUTINE USES'

Certain DoD "blanket routine uses" have been established that are applicable to every record system maintained by the Department of the Air Force, unless specifically stated otherwise within the particular record system notice. These additional routine uses of the records are published only once in the Air Force's Preamble to its compilation of records systems in the interest of simplicity, economy and to avoid redundancy.

##### *a. Law Enforcement Routine Use*

If a system of records maintained by a DoD Component to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

##### *b. Disclosure when Requesting Information Routine Use*

A record from a system of records maintained by a Component may be disclosed as a routine use to a federal, state, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a Component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

##### *c. Disclosure of Requested Information Routine Use*

A record from a system of records maintained by a Component may be disclosed to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

##### *d. Congressional Inquiries Routine Use*

Disclosure from a system of records maintained by a Component may be made to a congressional office from the record of an individual in response to an inquiry from the

congressional office made at the request of that individual.

*e. Private Relief Legislation Routine Use*

Relevant information contained in all systems of records of the Department of Defense published on or before August 22, 1975, will be disclosed to the Office of Management and Budget in connection with the review of private relief legislation as set forth in Office of Management and Budget Circular A-19 (reference (u)) at any stage of the legislative coordination and clearance process as set forth in that Circular.

*f. Disclosures Required by International Agreements Routine Use*

A record from a system of records maintained by a Component may be disclosed to foreign law enforcement, security, investigatory, or administrative authorities to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements including those regulating the stationing and status in foreign countries of DoD military and civilian personnel.

*g. Disclosure to State and Local Taxing Authorities Routine Use*

Any information normally contained in Internal Revenue Service (IRS) Form W-2 which is maintained in a record from a system of records maintained by a Component may be disclosed to state and local taxing authorities with which the Secretary of the Treasury has entered into agreements under 5 U.S.C., sections 5516, 5517, and 5520 (reference (v)) and only to those state and local taxing authorities for which an employee or military member is or was subject to tax regardless of whether tax is or was withheld. This routine use is in accordance with Treasury Fiscal Requirements Manual Bulletin No. 76-07.

*h. Disclosure to the Office of Personnel Management Routine Use*

A record from a system of records subject to the Privacy Act and maintained by a Component may be disclosed to the Office of Personnel Management (OPM) concerning information on pay and leave, benefits, retirement deduction, and any other information necessary for the OPM to carry out its legally authorized government-wide personnel management functions and studies.

*i. Disclosure to the Department of Justice for Litigation Routine Use*

A record from a system of records maintained by this component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee or member of the Depart-

ment in pending or potential litigation to which the record is pertinent.

*j. Disclosure to Military Banking Facilities Overseas Routine Use*

Information as to current military addresses and assignments may be provided to military banking facilities who provide banking services overseas and who are reimbursed by the Government for certain checking and loan losses. For personnel separated, discharged, or retired from the Armed Forces, information as to last known residential or home of record address may be provided to the military banking facility upon certification by a banking facility officer that the facility has a returned or dishonored check negotiated by the individual or the individual has defaulted on a loan and that if restitution is not made by the individual, the U.S. Government will be liable for the losses the facility may incur.

*k. Disclosure of Information to the General Services Administration (GSA) Routine Use*

A record from a system of records maintained by this component may be disclosed as a routine use to the General Services Administration (GSA) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

*l. Disclosure of Information to the National Archives and Records Administration (NARA) Routine Use*

A record from a system of records maintained by this component may be disclosed as a routine use to the National Archives and Records Administration (NARA) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

*m. Disclosure to the Merit Systems Protection Board Routine Use*

A record from a system of records maintained by this component may be disclosed as a routine use to the Merit Systems Protection Board, including the Office of the Special Counsel for the purpose of litigation, including administrative proceedings, appeals, special studies of the civil service and other merit systems, review of OPM or component rules and regulations, investigation of alleged or possible prohibited personnel practices; including administrative proceedings involving any individual subject of a DoD investigation, and such other functions, promulgated in 5 U.S.C. 1205 and 1206, or as may be authorized by law.

*n. Counterintelligence Purpose Routine Use*

A record from a system of records maintained by this component may be disclosed as a routine use outside the DoD or the U.S.

Government for the purpose of counterintelligence activities authorized by U.S. Law or Executive Order or for the purpose of enforcing laws, which protect the national security of the United States.

APPENDIX D TO PART 806b—GENERAL  
AND SPECIFIC EXEMPTIONS

(a) All systems of records maintained by the Department of the Air Force shall be exempt from the requirements of 5 U.S.C. 552a(d) pursuant to 5 U.S.C. 552a(k)(1) to the extent that the system contains any information properly classified under Executive Order 12958 and that is required by Executive Order to be kept classified in the interest of national defense or foreign policy. This exemption is applicable to parts of all systems of records including those not otherwise specifically designated for exemptions herein, which contain isolated items of properly classified information.

(b) An individual is not entitled to have access to any information compiled in reasonable anticipation of a civil action or proceeding (5 U.S.C. 552a(d)(5)).

(c) No system of records within Department of the Air Force shall be considered exempt under subsection (j) or (k) of the Privacy Act until the exemption rule for the system of records has been published as a final rule in the FEDERAL REGISTER.

(d) Consistent with the legislative purpose of 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.

(e) General Exemptions. The following systems of records claim an exemption under 5 U.S.C. 552a(j)(2), with the exception of F090 AF IG B, Inspector General Records and F051 AF JA F, Courts-Martial and Article 15 Records. They claim both the (j)(2) and (k)(2) exemption, and are listed under this part:

(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: F071 AF OSI D, Investigative Support Records.

(4) System identifier and name: F031 AF SP E, Security Forces Management Information System (SFMS).

(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. Therefore, portions of this system of records may be exempt pursuant to 5 U.S.C. 552a(j)(2) from the following subsections of 5 U.S.C. 552a(c)(3), (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).

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

(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 the following subsections of 5 U.S.C. 552a(c)(3), (c)(4), (d), (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 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.

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

(C) 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.

(D) From 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.

(E) From subsections (e)(4)(G) and (H) because this system of records is exempt from individual access pursuant to subsections (j)(2) of the Privacy Act of 1974.

(F) 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.

(G) 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 reporting on investigations and impede the development of intelligence necessary for effective law enforcement.

(H) 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.

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

(J) From subsection (g) because this system of records compiled for law enforcement

purposes and has been exempted from the access provisions of subsections (d) and (f).

(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. Therefore, portions of this system of records may be exempt pursuant to 5 U.S.C. 552a(j)(2) 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).

(B) 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. 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).

(ii) Authority: 5 U.S.C. 552a(j)(2) and (k)(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 ongoing 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) and (f).

(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 ongoing 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.

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

(i) Exemptions: (A) Parts of this system may be exempt pursuant to 5 U.S.C. 552a(j)(2) if the information is compiled and main-

tained by a component of the agency which performs as its principle function any activity pertaining to the enforcement of criminal laws. Therefore, 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).

(B) 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 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. 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).

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

(iii) Reason: (A) 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.

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

(C) 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.

(D) 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.

(E) 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.

(F) 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.

(G) 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.

(H) 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.

(I) 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.

(J) 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.

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

(L) 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).

(8) System identifier and name: F071 JTF A, Computer Network Crime Case System.

(i) Exemption: (A) Parts of this system 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. 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).

(B) 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 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. 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(j)(2) and (k)(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 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 ongoing 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.

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

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

(i) Exemption: Evaluation material used to determine potential for promotion in the Military Services may be exempt pursuant to 5 U.S.C. 552a(k)(7), but only to the extent that the disclosure of such material would reveal the identity of a confidential source. Therefore, portions of this system of records (Liaison Officer Evaluation and Selection Panel Candidate Evaluation) may be exempt pursuant to 5 U.S.C. 552a(k)(7) from the following subsections of 5 U.S.C. 552a(d), (e)(4)(H), and (f).

(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.

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

(i) Exemption: Testing or examination material used solely to determine individual qualifications for appointment or promotion in the federal or military service may be exempt pursuant to 5 U.S.C. 552a(k)(6), if the disclosure would compromise the objectivity or fairness of the test or examination process. Therefore, portions of this system of records may be exempt pursuant to 5 U.S.C. 552a(k)(6) from the following subsections of 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.

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

(i) Exemption: Evaluation material used to determine potential for promotion in the Military Services may be exempt pursuant to 5 U.S.C. 552a(k)(7), but only to the extent that the disclosure of such material would reveal the identity of a confidential source. Therefore, portions of this system of records may be exempt pursuant to 5 U.S.C. 552a(k)(7) from the following subsections of 5 U.S.C. 552a(d), (e)(4)(H), and (f).

(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.

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

(i) Exemption: 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. Therefore, portions of this system of records may be exempt pursuant to 5 U.S.C. 552a(k)(5) (Detachment Professional Officer Course Selection Rating Sheets; Air Force Reserve Officer Training Corps Form 0-24—Disenrollment Review; Memoranda for Record and Staff Papers with Staff Advice, Opinions, or Suggestions) may be exempt from the following subsections of 5 U.S.C. 552a(c)(3), (d), (e)(4)(G) and (H), and (f).

(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.

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

(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.

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

(i) Exemption: Evaluation material used to determine potential for promotion in the Military Services (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 pursuant to 5 U.S.C. 552a(k)(7), but only to the extent that the disclosure of such material would reveal the identity of a confidential source. Therefore, portions of this system of records may be exempt pursuant to 5 U.S.C. 552a(k)(7) from the following 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: (A) From 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.

(B) From subsection (d) because individual disclosure compromises express promises of confidentiality conferred to protect the integrity of the promotion rating system.

(C) From 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).

(D) From subsection (f) because of and to the extent that portions of this record system are exempt from the individual access provisions of subsection (d).

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

(i) Exemption: Evaluation material used to determine potential for promotion in the Military Services may be exempt pursuant to 5 U.S.C. 552a(k)(7), but only to the extent that the disclosure of such material would reveal the identity of a confidential source. Therefore, portions of this system of records may be exempt pursuant to 5 U.S.C. 552a(k)(7) from the following subsections of 5 U.S.C. 552a(c)(3), (d), (e)(4)(G), (H), and (I); and (f).

(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.

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

(i) Exemption: Evaluation material used to determine potential for promotion in the Military Services may be exempt pursuant to 5 U.S.C. 552a(k)(7), but only to the extent that the disclosure of such material would reveal the identity of a confidential source. Therefore, portions of this system of records

(Air Force General Officer Promotion and Effectiveness Reports with close out dates on or before January 31, 1991) may be exempt pursuant to 5 U.S.C. 552a(k)(7) may be exempt from following 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: (A) From 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.

(B) From subsection (d) because individual disclosure compromises express promises of confidentiality conferred to protect the integrity of the promotion rating system.

(C) From 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).

(D) From subsection (f) because of and to the extent that portions of this record system are exempt from the individual access provisions of subsection (d).

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

(i) Exemption: Testing or examination material used solely to determine individual qualifications for appointment or promotion in the federal or military service, if the disclosure would compromise the objectivity or fairness of the test or examination process may be exempt pursuant to 5 U.S.C. 552a(k)(6), if the disclosure would compromise the objectivity or fairness of the test or examination process. Therefore, portions of this system of records may be exempt pursuant to 5 U.S.C. 552a(k)(6) from the following subsections of 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. Reserved.

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

(i) Exemption: 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. Therefore, portions of this system of records 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), (e)(4)(G), (H), and (I), and (f).

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

(iii) Reasons: To protect those who gave information in confidence during Air Force Of-

fice of Special Investigations 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 Air Force Office of Special Investigations personnel program that relies on selecting only qualified people.

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

(i) Exemptions: Evaluation material used to determine potential for promotion in the Military Services may be exempt pursuant to 5 U.S.C. 552a(k)(7), but only to the extent that the disclosure of such material would reveal the identify of a confidential source. Therefore, portions of this system of records may be exempt pursuant to 5 U.S.C. 552a(k)(7) from the following subsections of 5 U.S.C. 552a(d), (e)(4)(H), and (f).

(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.

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

(i) Exemption: (A) 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 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) 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.

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

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

(iii) Reasons: To protect the identity of sources to which 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.

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

(i) Exemption: 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. Therefore, portions of this system of records 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), (e)(4)(G), (H), and (I), and (f).

(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.

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

(i) Exemption: 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. Therefore, portions of this system of records 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), (e)(4)(G), (H), and (I), and (f).

(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.

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

(i) Exemption: 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. Therefore, portions of this system of records 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), (e)(4)(G), (H), and (I), and (f).

(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.

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

(i) Exemption: 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. Therefore, portions of this system of records may be exempt pursuant to 5 U.S.C. 552a(k)(5) from the following subsection of 5 U.S.C. 552a(d).

(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.

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

(i) Exemption: 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. 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(d), (e)(4)(H), and (f).

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

(iii) Reasons: (A) 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.

(B) 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.

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

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

(i) Exemption: 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. 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.

(19) [Reserved]

(20) 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.

(21) 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.

(22) System identifier and name: F051 AFJA E, Judge Advocate General's Professional Conduct Files.

(i) *Exemption:* 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, 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 investigatory reports maintained in a system of records used in personnel or administrative actions. 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.

(23) System identifier and name F033 USSC A, Information Technology and Control Records.

(i) *Exemption:* 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, 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. 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.

(24) System identifier and name: F036 AETC X, College Scholarship Program.

(i) *Exemption:* Investigatory material compiled solely for the purpose of determining suitability \* \* \* the identity of a confidential source. 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) and 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.

(25) System identifier and name: F032 AFCEA C, Civil Engineer System-Explosive Ordnance Records.

(i) *Exemption:* Records maintained in connection with providing protective services to the President and other individuals under 18 U.S.C. 3056, may be exempt pursuant to 5 U.S.C. 552a(k)(3) 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)(3).

(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.

(26) System identifier and name: F051 AF JAA, Freedom of Information Appeal Records.

(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 na-

tional 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.

[69 FR 954, Jan. 7, 2004, as amended at 69 FR 12540, Mar. 17, 2004; 70 FR 46405, Aug. 10, 2005; 74 FR 55785, 55786, 55787, 55788, Oct. 29, 2009; 74 FR 57415, Nov. 6, 2009]

## APPENDIX E TO PART 806b—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. The Privacy Impact Assessment 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 Privacy Impact Assessment.

(3) Define the privacy issues you will address in the Privacy Impact Assessment.

(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 100-503, The Computer Matching and Privacy Act of 1988.<sup>13</sup>

(2) Public Law 100-235, The Computer Security Act of 1987,<sup>14</sup> which establishes minimum security practices for Federal computer systems.

(3) OMB Circular A-130, Management of Federal Information Resources,<sup>15</sup> which provides instructions to Federal agencies on how to comply with the fair information practices and security requirements for operating automated information systems.

(4) Public Law 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) DoD Directive 5400.11, Department of Defense Privacy Program,<sup>16</sup> December 13, 1999.

(7) DoD 5400.11-R, Department of Defense Privacy Program,<sup>17</sup> August 1983.

(8) Air Force Instruction 33-332, Air Force Privacy Act Program.

(c) The Air Force Privacy Office is in the Office of the Air Force Chief Information Officer, 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. Air Force Chief Information Officer is requiring the use of this Privacy Impact Assessment in order to ensure that the systems the Air Force develops protect individuals' privacy. The Privacy Impact Assessment incorporates privacy into the development life cycle so that all system development initiatives can appropriately con-

sider privacy issues from the earliest stages of design.

(a) What is a Privacy Impact Assessment? The Privacy Impact Assessment 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 Privacy Impact Assessment process is described in detail in Section C, Completing a Privacy Impact Assessment.

(b) When is a Privacy Impact Assessment Done? The Privacy Impact Assessment 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 Privacy Impact Assessment? Both the system owner and system developers must work together to complete the Privacy Impact Assessment. 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 Privacy Impact Assessment? Accomplish Privacy Impact Assessments when:

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

(2) Initiating a new collection of information, using information technology, 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 Major Command Privacy Act Officer reserves the right to request that a Privacy Impact Assessment be completed on any system that may have privacy risks.

#### *Section C—Completing a Privacy Impact Assessment*

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

Training. Training on the Privacy Impact Assessment will be available, on request,

<sup>13</sup> [http://www.defenselink.mil/privacy/1975OMB\\_PAGuide/jun1989.pdf](http://www.defenselink.mil/privacy/1975OMB_PAGuide/jun1989.pdf).

<sup>14</sup> [http://csrc.nist.gov/secplcy/csa\\_87.txt](http://csrc.nist.gov/secplcy/csa_87.txt).

<sup>15</sup> <http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html>.

<sup>16</sup> <http://www.dtic.mil/whs/directives/corres/html/540011.htm>.

<sup>17</sup> <http://www.dtic.mil/whs/directives/corres/html/540011r.htm>.

from the Major Command Privacy Act Officer. The training consists of describing the Privacy Impact Assessment process and provides detail about the privacy issues and privacy questions to be answered to complete the Privacy Impact Assessment. Major Command Privacy Act Officers may use appendix E, Sections A, B, D, and E for this purpose. The intended audience is the personnel responsible for writing the Privacy Impact Assessment document.

The Privacy Impact Assessment Document. Preparing the Privacy Impact Assessment 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 Privacy Impact Assessment

document, the Major Command Privacy Act Officer will be available to answer questions related to the Privacy Impact Assessment process and other concerns that may arise with respect to privacy.

Review of the Privacy Impact Assessment Document. Submit the completed Privacy Impact Assessment document to the Major Command Privacy Act Office for review. The purpose of the review is to identify privacy risks in the system.

Approval of the Privacy Impact Assessment. 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. Major Command and Headquarters Air Force Functional CIOs will issue final approval of the Privacy Impact Assessment.

TABLE A4.1—OUTLINE OF STEPS FOR COMPLETING A PRIVACY IMPACT ASSESSMENT

Step	Who	Procedure
1 .....	System Owner, and Developer .....	Request and complete Privacy Impact Assessment Training.
2 .....	System Owner, and Developer .....	Answer the questions in Section E, Privacy Questions. For assistance contact your Major Command Privacy Act Officer.
3 .....	System Owner, and Developer .....	Submit the Privacy Impact Assessment document to the Major Command Privacy Act Officer.
4 .....	Major Command Privacy Act Officer .....	Review the Privacy Impact Assessment document to identify privacy risks from the information provided. The Major Command Privacy Act Officer will get clarification from the owner and developer as needed.
5 .....	System Owner and Developer, Major Command Privacy Act Officer.	The System Owner, Developer and the Major Command Privacy Act Officer should reach agreement on design requirements to resolve all identified risks.
6 .....	System Owner, Developer, and Major Command 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 Major Command or Headquarters Air Force Functional CIO.
7 .....	Major Command or Headquarters Air Force Functional CIO.	Issue final approval of Privacy Impact Assessment, and send a copy to Air Force Chief Information Officer/P.
8 .....	Air Force Chief Information Officer/P .....	When feasible, publish Privacy Impact Assessment on Freedom of Information Act Web page ( <a href="http://www.foia.af.mil">http://www.foia.af.mil</a> ).

*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 and disposal procedures and coordinate them with the Major Command Records Manager.

*Section E—Privacy Questions*

## Data in the System

1. Generally describe the information to be used in System 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 Data (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 Data 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 a personal identifier? If yes, explain.

## Maintenance of Administrative Controls

- (1) a. Explain how the system and its use will ensure Administrative 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 Major 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?

## Department of the Air Force, DoD

## § 807.3

(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.

### PART 807—SALE TO THE PUBLIC

Sec.

807.1 General requirements.

807.2 Charges for publications and forms.

807.3 Requests for classified material, For Official Use Only material, accountable forms, storage safeguard forms, Limited (L) distribution items, and items with restrictive distribution caveats.

807.4 Availability and nonavailability of stock.

807.5 Processing requests.

807.6 Depositing payments.

AUTHORITY: 10 U.S.C. 8013.

SOURCE: 55 FR 36631, Sept. 6, 1990, unless otherwise noted.

#### § 807.1 General requirements.

(a) Unaltered Air Force publications and forms will be made available to the public with or without charge, subject to the requirements of this part. Base Chiefs of Information Management will set up procedures to meet these needs and will make available Master Publications Libraries for public use according to AFR 4-61. They will also advise requesters that these libraries are available, since in many cases this will satisfy their needs and reduce workloads in processing sales requests. If the item is on sale by the Superintendent of Documents, GPO, refer the request to that outlet. Refer general public requests for Air Force administrative publications and forms to the National Technical Information Service (NTIS), Defense Publication Section, US Department of Commerce, 4285 Port Royal Road, Springfield, VA 22161-0001.

(b) The Air Force does not consider these unaltered publications and forms as records, within the meaning of the Freedom of Information Act (FOIA), as outlined in 5 U.S.C. 552 and implemented by part 806 of this chapter. Refer requests that invoke the FOIA to the chief, base information management, for processing.

(c) Units will process requests under the Foreign Military Sales Program

(FMS) as specified in AFR 4-71, chapter 11.

(d) Units will send requests from foreign governments, their representatives, or international organizations to the MAJCOM foreign disclosure policy office and to HQ USAF/CVAII, Washington DC 20330-5000. Also send information copies of such requests to the base public affairs office. Commands will supplement this requirement to include policies pertaining to those items for which they have authority to release.

(e) Units will return a request for non-Air Force items to the requester for submission to appropriate agency.

#### § 807.2 Charges for publications and forms.

(a) The Air Force applies charges to all requests unless specifically excluded.

(b) The Air Force applies charges according to part 813, Schedule of Fees for Copying, Certifying, and Searching Records and Other Documentary Material. Additional guidance is in part 812, User Charges, including specific exclusion from charges as listed in § 812.5. As indicated, the list of exclusions is not all inclusive and recommendations for additional exclusions are sent to the office of primary responsibility for part 812 of this chapter.

(c) When a contractor requires publications and forms to perform a contract, the Air Force furnishes them without charge, if the government contracting officer approves these requirements.

#### § 807.3 Requests for classified material, For Official Use Only material, accountable forms, storage safeguard forms, Limited (L) distribution items, and items with restrictive distribution caveats.

(a) *Classified material.* The unit receiving the requests should tell the requester that the Air Force cannot authorize the material for release because it is currently and properly classified in the interest of national security as authority by Executive Order, and must be protected from unauthorized disclosure.

(b) *For Official Use Only (FOUO) material.* The office of primary responsibility for the material will review

## § 807.4

these requests to determine the material's releasability.

(c) *Accountable forms.* The unit receiving the request will return it to the requester stating that the Air Force stringently controls these forms and cannot release them to unauthorized personnel since their misuse could jeopardize Department of Defense security or could result in fraudulent financial gain or claims against the government.

(d) *Storage safeguard forms.* The unit receiving these requests returns them to the requesters stating that the Air Force specially controls these forms and that they are not releasable outside the Department of Defense since they could be put to unauthorized or fraudulent use.

(e) Limited (L) distribution items are not releasable outside the Department of Defense without special review according to AFR 700-6. Units receiving these requests should refer them to the SCS manager shown in the index or on the cover of the publications. Advise the requesters of the referral.

(f) *Items with restrictive distribution caveats.* Some publications have restrictive distribution caveats on the cover. Follow the instructions stated and advise the requesters of the referral.

## § 807.4 Availability and nonavailability of stock.

(a) Limit quantities furnished so that stock levels required for operational Air Force support are not jeopardized.

(b) If the item is not available from publishing distribution office (PDO) stock, obtain it from the Air Force Publishing Distribution Center. If the item is under revision, advise the requester that it is being revised and that no stock is available.

(c) If stocks are not available and the item is being reprinted, advise the requester that stocks are expected to be available in 90 calendar days and to resubmit at that time.

## § 807.5 Processing requests.

Payment is required before shipping the requested material. Payment must be by check or money order.

(a) Upon receipt of the request, determine the cost involved and request the material.

## 32 CFR Ch. VII (7-1-12 Edition)

(b) Upon receipt of the item, advise the requester to resubmit the required payment and send the material after payment is received.

(c) If the material cannot be obtained, advise the requester of the reason.

## § 807.6 Depositing payments.

Obtain instructions from the local Accounting and Finance Office regarding how checks or money orders must be prepared and required procedures for depositing them.

## PART 809a—INSTALLATION ENTRY POLICY, CIVIL DISTURBANCE INTERVENTION AND DISASTER ASSISTANCE

Sec.

809a.0 Purpose.

### Subpart A—Installation Entry Policy

809a.1 Random installation entry point checks.

809a.2 Military responsibility and authority.

809a.3 Unauthorized entry.

809a.4 Use of Government facilities.

809a.5 Barment procedures.

### Subpart B—Civil Disturbance Intervention and Disaster Assistance

809a.6 Authority.

809a.7 Definitions.

809a.8 Installation policies and laws.

809a.9 Conditions for use of Air Force resources.

809a.10 Military commanders' responsibilities.

809a.11 Procedures outside the United States.

AUTHORITY: 10 U.S.C. 332 and 333.

SOURCE: 67 FR 13718, Mar. 26, 2002, unless otherwise noted.

## § 809a.0 Purpose.

This part prescribes the commanders' authority for enforcing order within or near Air Force installations under their jurisdiction and controlling entry to those installations. It provides guidance for use of military personnel in controlling civil disturbances and in supporting disaster relief operations. This part applies to installations in the

United States, its territories and possessions, and will be used to the maximum extent possible in the overseas commands. Instructions issued by the appropriate overseas commander, status of forces agreements, and other international agreements provide more definitive guidance for the overseas commands. Nothing in this part should be construed as authorizing or requiring security forces units to collect and maintain information concerning persons or organizations having no affiliation with the Air Force other than a list of persons barred from the installation.

### Subpart A—Installation Entry Policy

#### § 809a.1 Random installation entry point checks.

The installation commander determines when, where, and how to implement random checks of vehicles or pedestrians. The commander conducts random checks to protect the security of the command or to protect government property.

#### § 809a.2 Military responsibility and authority.

(a) Air Force installation commanders are responsible for protecting personnel and property under their jurisdiction and for maintaining order on installations, to ensure the uninterrupted and successful accomplishment of the Air Force mission.

(b) Each commander is authorized to grant or deny access to their installations, and to exclude or remove persons whose presence is unauthorized. In excluding or removing persons from the installation, the installation commander must not act in an arbitrary or capricious manner. Their action must be reasonable in relation to their responsibility to protect and to preserve order on the installation and to safeguard persons and property thereon. As far as practicable, they should prescribe by regulation the rules and conditions governing access to their installation.

#### § 809a.3 Unauthorized entry.

Under Section 21 of the Internal Security Act of 1950 (50 U.S.C. 797), any

directive issued by the commander of a military installation or facility, which includes the parameters for authorized entry to or exit from a military installation, is legally enforceable against all persons whether or not those persons are subject to the Uniformed Code of Military Justice (UCMJ). Military personnel who reenter an installation after having been properly ordered not to do so may be apprehended. Civilian violators may be detained and either escorted off the installation or turned over to proper civilian authorities. Civilian violators may be prosecuted under 18 U.S.C. 1382.

#### § 809a.4 Use of Government facilities.

Commanders are prohibited from authorizing demonstrations for partisan political purposes. Demonstrations on any Air Force installation for other than political purposes may only occur with the prior approval of the installation commander. Demonstrations that could result in interference with, or prevention of, the orderly accomplishment of the mission of an installation or that present a clear danger to loyalty, discipline or morale of members of the Armed Forces will not be approved.

#### § 809a.5 Barment procedures.

Under the authority of 50 U.S.C. 797, installation commanders may deny access to the installation through the use of a barment order. Barment orders should be in writing but may also be oral. Security forces maintain a list of personnel barred from the installation.

### Subpart B—Civil Disturbance Intervention and Disaster Assistance

#### § 809a.6 Authority.

The authority to intervene during civil disturbances and to provide disaster assistance is bound by directives issued by competent authorities. States must request federal military intervention or aid directly from the President of the United States by the state's legislature or executive. Installation commanders must immediately report these requests in accordance with AFI 10-802, *Military Support to*

## § 809a.7

*Civil Authorities* (Available from National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.).

### § 809a.7 Definitions.

The following definitions apply to this part:

(a) *Emergencies*. These are conditions which affect public welfare and occur as a result of enemy attack, insurrection, civil disturbances, earthquake, fire, flood, or other public disasters which endanger life and property or disrupt the usual process of government. The term "emergency" includes any or all of the conditions explained in this section.

(b) *Civil defense emergency*. This is a disaster situation resulting from devastation created by an enemy attack and requiring emergency operations during and following attack. It may also be proclaimed by appropriate authority in anticipation of an attack.

(c) *Civil disturbances*. These are group acts of violence or disorder prejudicial to public law and order including those which follow a major disaster. They include riots, acts of violence, insurrections, unlawful obstructions or assemblages, or other disorders.

(d) *Major disaster*. Any flood, fire, hurricane, or other catastrophe which, in the determination of the President, is or threatens to be of sufficient severity and magnitude to warrant disaster assistance by the Federal Government to supplement the efforts and available resources of the State and local governments in alleviating the damage, hardship, or suffering caused thereby.

### § 809a.8 Installation policies and laws.

This subpart contains policies on the use of Air Force military personnel in civil disturbances and disasters. The more important laws concerning military aid to civil authorities are also summarized.

(a) The Air Force gives military assistance to civil authorities in civil defense or civil disturbances and disasters only when such assistance is requested or directed. Commanders will not undertake such assistance without authority, unless the overruling demands of humanity compel immediate

## 32 CFR Ch. VII (7-1-12 Edition)

action to protect life and property and to restore order.

(b) The military service having available resources nearest the affected area is responsible for providing initial assistance to civil authorities in emergencies. Subsequent operations are to be according to the mutual agreement between the senior service commanders concerned.

(c) The protection of life and property and the maintenance of law and order within the territorial jurisdiction of any State is the primary responsibility of State and local authorities. It is well-established U.S. Government policy that intervention with military forces takes place only after State and local authorities have used their own forces and are unable to control the situation, or when they do not take appropriate action.

### § 809a.9 Conditions for use of Air Force resources.

This part is not intended to extend Air Force responsibilities in emergencies to generate additional resources (manpower, materiel, facilities, etc.) requirements, or encourage participation in such operations at the expense of the Air Force primary mission. It is a guide for the employment of Air Force resources when:

(a) A disaster or disturbance occurs in areas in which the U.S. Air Force is the executive agent of the United States.

(b) A disaster or disturbance occurs in areas that are remote from an Army installation but near an Air Force installation, thereby necessitating Air Force assumption of responsibility pending arrival of Army personnel.

(c) The overriding demand of conditions resulting from a natural disaster compels immediate action to protect life and property and to restore order.

### § 809a.10 Military commanders' responsibilities.

(a) Civilians in the affected area will be informed of the rules of conduct and other restrictive measures to be enforced by the military. These will be announced by local proclamation or order, and will be given the widest publicity by all available media.

**Department of the Air Force, DoD**

**§ 809a.11**

(b) Persons not normally subject to military law, who are taken into custody by military forces incident to civil disturbances, will be turned over to the civil authorities as soon as possible.

(c) Military forces will ordinarily exercise police powers previously inoperative in an affected area; restore and maintain order; maintain essential transportation and communication; and provide necessary relief measures.

(d) U.S. Air Force civilian employees may be used, in any assignments in which they are capable and willing to serve. In planning for on-base contingencies of fires, floods, hurricanes, and other natural disasters, arrangements should be made for the identification and voluntary use of individual em-

ployees to the extent that the needs for their services are anticipated.

**§ 809a.11 Procedures outside the United States.**

It is Air Force policy to make every reasonable effort to avoid any confrontation between United States military forces and host nation demonstrators or other dissidents posing a threat to Air Force resources. Intervention by United States military personnel outside the United States is governed by international law, bilateral and other international agreements to which the United States is a party, and host-nation laws. Local plans to counter such situations must include provisions to request and obtain host nation civil or military support as quickly as possible.