

prior order for the Minneapolis-St. Paul area.

Many of the producers who were brought under the merged order, particularly those in Wisconsin, had been accustomed to receiving payments 15 days apart. They preferred such payments to being paid on the 18th and 25th of the month. To accommodate this, the pertinent provisions of the order have been suspended since November 1976 (41 FR 51389, 42 FR 22360, 42 FR 59747, and 43 FR 19341). As requested, the suspensions were limited to payments to producers for whom a cooperative was not collecting payments.

A continuation of the suspension through April 1980 is supported by a cooperative association, the operator of a pool distributing plant and by a producer. The pool plant operator indicated that his producers desire receiving payment for their milk on the 3rd and 18th days of the following month. He claimed that assignments against the milk checks of producers are set to correspond with these dates and that any change in them would cause a bookkeeping problem for the producers.

The producer indicated that he would prefer receiving his payment about every 15 days. This, he claimed, would allow him to save interest expense on his feed supplies and on his farm mortgage. With respect to feed supplies, he stated that he receives a credit from his supplier if payment is made in full within 5 days after delivery. He also stated that payments every 15 days would allow him to save 5-7 days interest each month on his farm mortgage because interest is compounded daily.

The suspension should be extended for an additional period of twelve months pending a hearing at which proposals to amend the partial payment provisions may be considered. The suspension will enable handlers to continue to accommodate their producers who request that their payments be spaced about 15 days apart.

It is hereby found and determined that thirty days' notice of the effective date hereof is impractical, unnecessary, and contrary to the public interest in that the suspension does not require of persons affected substantial or extensive preparation prior to the effective date and notice of proposed rulemaking was given interested parties and they were afforded opportunity to file written data, views or arguments concerning the suspension.

Therefore, good cause exists for making this order effective May 1, 1979.

It is therefore ordered, That the aforesaid provisions of the order are hereby suspended for the months of May 1979 through April 1980.

(Secs. 1-19, 48 Stat. 31 as amended; 7 U.S.C. 601-674)

Effective date: May 1, 1979.

Signed at Washington, D.C., on April 12, 1979.

P. R. "Bobby" Smith,

Assistant Secretary for Marketing and Transportation Services.

[Milk Order 68]

[FR Doc. 79-12019 Filed 4-17-79; 8:45 am]

BILLING CODE 3410-02-M

TENNESSEE VALLEY AUTHORITY

18 CFR Part 304

Amendments to Regulations Governing Approval of Construction and Regulation of Structures on the Tennessee River System

AGENCY: Tennessee Valley Authority (TVA).

ACTION: Final rule.

SUMMARY: This rule changes the existing delegations of authority by the Board of Directors of the Tennessee Valley Authority (TVA) in connection with the approval of construction in the Tennessee River system and regulation of structures. It delegates to the Director of Land and Forest Resources and the Division of Land and Forest Resources, respectively, all functions and responsibilities under 18 CFR Part 304 formerly delegated to the Director of Property and Services and the Division of Property and Services.

EFFECTIVE DATE: April 18, 1979.

FOR FURTHER INFORMATION CONTACT: Richard L. Morgan, Jr., Director of Land and Forest Resources, Forestry Building, Norris, Tennessee 37828 (615-632-4411).

SUPPLEMENTARY INFORMATION: A recent reorganization of TVA's offices and divisions includes the transfer to the Division of Land and Forest Resources in the Office of Natural Resources the land management functions for which the Division of Property and Services was formerly responsible, including the review and initial approval or disapproval under Section 26a of the Tennessee Valley Authority Act of 1933, as amended (16 U.S.C. 831y-1 (1976)), of plans for structures in the Tennessee River system. The changes made by this rule in the delegation of power to approve or disapprove such plans and administration of the handling of applications for such approval reflect this aspect of the reorganization and

simply transfer to the Director and Division of Land and Forest Resources all of the powers and responsibilities under 18 CFR Part 304 formerly vested in the Director and Division of Property and Services.

Accordingly 18 CFR Part 304 is amended as follows:

1. Section 304.1 is amended by changing the definition of Director to read:

§ 304.1 Definitions.

Except as the context may otherwise require, the following words or terms, when used in this Part 304, have the meaning specified in this section.

"Director" means the Director of Land and Forest Resources of TVA.

2. Section 304.101 is amended to read:

§ 304.101 Delegation of authority.

The power to approve or disapprove applications under this part is delegated to the Director, subject to appeal to the Board as provided in § 304.106. In his discretion the Director may submit any application to the Board for its approval or disapproval. Administration of the handling of applications is delegated to the Division of Land and Forest Resources.

3. Section 304.102 is amended to read:

§ 304.102 Application.

Applications shall be addressed to Tennessee Valley Authority, Director of Land and Forest Resources, Norris, Tennessee 37828.

4. Section 304.103 is amended by revising the first sentence of paragraph (c) to read:

§ 304.103 Contents of application.

(c) Detailed information concerning contents of applications, kinds and amounts of information required to be submitted for specific structures, and instructions are available at the address specified in § 304.102 or from the Manager of Properties, Division of Land and Forest Resources, Tennessee Valley Authority, at one of the following district offices:

5. Section 304.105 is amended by revising paragraph (a) to read:

§ 304.105 Determination of application.

(a) The Division of Land and Forest Resources conducts preliminary investigations; coordinates the processing of applications within TVA; notifies the applicant if preparation and review of an environmental statement

are required under NEPA and of what additional information must be submitted to TVA by applicant so that TVA may comply with the requirements of that statute and related legal requirements, and complete its review of the application; and arranges for notification to the Environmental Protection Agency of applications that request approval of plans for structures which may result in a discharge into navigable waters of the United States and are certified in accordance with the requirements of § 304.103(b).

* * * * *

(16 U.S.C. 831-831dd)

Note.—TVA has determined that the amendments of 18 CFR Part 304 contained in this document are not significant within the meaning of Executive Order No. 12044 and under TVA's criteria established pursuant thereto.

Dated: April 5, 1979.

Leon E. Ring,

General Manager.

[FR Doc. 79-11971 Filed 4-17-79; 8:45 am]

BILLING CODE 8120-01-M

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

Office of Assistant Secretary for Housing—Federal Housing Commissioner

24 CFR Part 207

Multifamily Housing Mortgage Insurance; Mortgagee's Late Charge

AGENCY: Department of Housing and Urban Development.

ACTION: Correction of final rule.

SUMMARY: On December 26, 1978, at 43 FR 60154, the Secretary adopted an amendment to 24 CFR Part 207. Reference was made to a new § 207.252c. Since 24 CFR Part 207 already had a § 207.252c, this reference should have been § 207.252d.

EFFECTIVE DATE: December 26, 1978.

FOR FURTHER INFORMATION CONTACT: T. J. O'Connor, Director, Office of Finance and Accounting, Room 2202, Telephone 202-755-6310 (This is not a toll free number).

Accordingly, 24 CFR Part 207 is amended as follows, effective as of December 26, 1978, the date the final rule was published:

Subpart B—Contract Rights and Obligations

1. The table of contents to Part 207 is amended to add a reference to a new

§ 207.252d and designated "Mortgagee's late charge."

2. A new § 207.252d is added to read as follows:

§ 207.252d Mortgagee's late charge.

* * * * *

(Sec. 7(d), Department of Housing and Urban Development Act (42 U.S.C. 3535(d)).)

Issued at Washington, D.C., April 4, 1979.

Morton Baruch,

Deputy Assistant Secretary for Housing—Federal Housing Commissioner.

[Docket R-79-527]

[FR Doc. 79-11967 Filed 4-17-79; 8:45 am]

BILLING CODE 4210-01-M

24 CFR Part 232

Nursing Homes and Intermediate Care Facilities Mortgage Insurance

AGENCY: Department of Housing and Urban Development (HUD).

ACTION: Final rule.

SUMMARY: This final rule amends Part 232 with respect to leases executed by a governmental agency, an Indian, an Indian tribe, or such other lessor as the Commissioner may approve.

EFFECTIVE DATE: May 18, 1979.

FOR FURTHER INFORMATION CONTACT:

Charles P. Storrs, Jr., Office of Multifamily Development, Room 6116, Department of Housing and Urban Development, Washington, D.C. 20410, (202) 755-9280 (This is not a toll-free number).

SUPPLEMENTARY INFORMATION: The property requirements in Part 207 of the regulations allow a lease executed by a governmental agency, an Indian, an Indian tribe, or such other lessor that the Commissioner may approve with a term of not less than 50 years to run from the date the mortgage is executed. This provision is contained in the regulations for the Section 207 program, the basic multifamily housing program.

It now becomes necessary to amend Part 232 to include this 50-year leasehold term provision in the nursing home program in order to provide nursing home mortgage insurance to benefit Indian tribes and others. A 50-year leasehold term is the maximum that an Indian tribe may acquire in certain instances, and the present Section 232 requirement of 55 years would exclude most Indian tribes from participating in the program.

Since this amendment would provide a benefit to certain Indian tribes and since it is in the public interest to provide such benefit without delay, the Secretary has found that the delay that would result from notice and public

procedure would be contrary to the public interest. Accordingly, a public comment period is not required, and this amendment is published as a final rule.

A finding of inapplicability respecting the National Environmental Policy Act of 1969 has been made in accordance with HUD procedures. A copy of this finding of inapplicability will be available for public inspections during regular business hours at the Office of the Rules Docket Clerk, Office of the General Counsel, Room 5218, Department of Housing and Urban Development, 451 Seventh Street, S.W., Washington, D.C. 20410.

Accordingly, Part 232 is amended by adding a new paragraph (d) to Section 232.25a, to read as follows:

§ 232.25a Eligibility of property.

* * * * *

(c) * * * ; or

(d) Under a lease executed by a governmental agency, an Indian, an Indian tribe, or such other lessor as the Commissioner may approve for the maximum term consistent with the legal authority for the execution of such lease, provided that the term of any such lease shall run for a period of not less than 50 years from the date the mortgage is executed.

* * * * *

Issued at Washington, D.C., April 6, 1979.

Morton Baruch,

Deputy Assistant Secretary for Housing—Federal Housing Commissioner.

[Docket No. R 79-647].

[FR Doc. 79-11968 Filed 4-17-79; 8:45 am]

BILLING CODE 4210-01-M

DEPARTMENT OF DEFENSE

Department of the Air Force

32 CFR Part 806b

Air Force Privacy Act Program

AGENCY: Department of the Air Force, Department of Defense.

ACTION: Final rule.

SUMMARY: The Department of the Air Force has rewritten its rules for the operation of the Air Force Privacy Act program to reduce their length and complexity. The structure of the rules has been reorganized to follow the process of information collection, maintenance and dissemination. In addition, a section on fees and one on training has been added. This revision is intended to make the program more understandable to persons seeking access to records on themselves which the Air Force is maintaining. It is also

intended to reduce operating costs and improve responsiveness by giving program managers clear and logical instructions on how to operate the program. Except for revising the text, however, these rules do not alter practices and procedures already in effect.

EFFECTIVE DATE: April 11, 1979.

FOR FURTHER INFORMATION CONTACT: Captain Robert N. Veeder, Chief, Air Force Privacy Act Office, HQ USAF/DAAD(S), Washington, D.C. 20330, phone: 202-694-3431.

SUPPLEMENTARY INFORMATION: On February 5, 1979, the Department of the Air Force published a proposed rule (44 FR 6944) to revise Part 806b at 32 CFR, Air Force Privacy Act Program. As stated at that time, the revision adds decision logic tables for processing requests, appeals, time limits, and disclosure accounting and consent requirements; designates the Chief, Office of Civilian Personnel as Denial Authority for civilian records; transfers subpart on Privacy Act requirements for forms and regulations to Forms Management Office and Publications Management Office; and adds a subpart on training. Interested persons were invited to participate in the proposed rulemaking change. Since no public comments were received prior to the expiration date for public comment, Part 806b is revised to read as follows:

PART 806b—AIR FORCE PRIVACY ACT PROGRAM

Sec.

806b.0 Purpose.

Subpart A—General Information

- 806b.1 Air Force policy.
- 806b.2 Terms explained.
- 806b.3 Air Force supplements.
- 806b.4 Responsibilities assigned.
- 806b.5 Delegation of authority.
- 806b.6 Judicial sanctions.

Subpart B—Collecting Personal Information

- 806b.7 Collecting from the individual.
- 806b.8 Privacy Act statements.
- 806b.9 Promises of confidentiality when collecting information about individuals from third parties.

Subpart C—Maintaining Information in Systems of Records

- 806b.10 Air Force standards.
- 806b.11 Protecting records.
- 806b.12 Public notice and reporting requirements.
- 806b.13 Evaluating systems of records.

Subpart D—Disclosing Information from Systems of Records

- 806b.14 Disclosures to the subjects of records.

806b.15 Disclosures of third parties and organizations.

Subpart E—Exempting Systems of Records

- 806b.16 Exemption index and cross reference.
- 806b.17 General exemptions.
- 806b.18 Specific exemptions.

Subpart F—Other Administrative Actions

- 806b.19 Training.
- 806b.20 Annual Privacy Act Report, RCS: DD-A(A&AR) 1379.
- 806b.21 Systems Notice Requirements.
- 806b.22 General and specific exemptions claimed.

Authority: 5 U.S.C. 552, as amended by Pub. L. 93-501.

Note: This part is derived from Air Force Regulation 12-35, April 11, 1979. Part 806 of this chapter states the basic policies and instructions governing the disclosure of records and tells members of the public what they must do to inspect or obtain copies of the material referenced herein.

§ 806b.0 Purpose.

This part explains policies and outlines procedures that govern collecting personal information and safeguarding, maintaining, using, accessing, amending, and disseminating personal information kept by the Department of the Air Force in systems of records. It implements 5 U.S.C. 552a, Pub. L. 93-579 and DOD Directive 5400.11, August 4, 1975. It is published in Title 32 CFR 806b and applies to all Air Force activities, including the Reserve Components, except for the office of the Chief, National Guard Bureau; Air National Guard technicians; and Army-Air Force Exchange Service activities, including Motion Picture Service Activities. It does not apply to civilian employee records which are maintained by Air Force activities and are covered under the Civil Service Government-wide systems of records, reprinted in AFP 12-36, Part Three. Such records are subject to Parts 293, 294, and 297 of Civil Service Commission regulations and the Federal Personnel Manual and Air Force Supplements. In case of a conflict, this part takes precedence over any existing Air Force directive that deals with the personal privacy and rights of individuals regarding their personal records, except for disclosures of personal information required by the Freedom of Information Act (FOIA), 5 U.S.C. 552, as amended by Pub. L. 93-502 and implemented by AFR 12-30.

Subpart A—General Information

§ 806b.1 Air Force policy.

It is Air Force policy to:

- (a) Protect the privacy of individuals from unwarranted invasion as required by the Privacy Act of 1974.

Individuals covered by this protection are living citizens of the United States or aliens lawfully admitted for permanent residence. A legal guardian or parent has the same rights as, and may act on behalf of, a minor. (A member of the Armed Forces is not a minor for the purposes of this part.)

(b) Collect, keep, and use only that personal information needed to support Air Force operations and programs as authorized by law or Executive Order. Disclose this information only as authorized by the Privacy Act of 1974 and this part.

(c) Keep only that personal information that is timely, accurate, complete, and relevant to the purpose for which it was collected.

(d) Safeguard personal information to prevent unauthorized use, disclosure, alteration, or destruction.

(e) Let individuals know what records the Air Force is keeping on them, and to let them review or get copies of these records, subject to exemption procedures authorized by law and published in this part.

(f) Let individuals amend records about themselves that they can prove are in error, or are untimely, incomplete, or irrelevant.

(g) Let individuals ask for an administrative review of decisions that deny them access to, or do not let them amend, their records.

(h) Keep personal information only for as long as it is needed to protect the rights of the citizen and the Government, and to provide for the administrative needs of the Air Force.

§ 806b.2 Terms explained.

Terms, and their meanings, used in this part are:

(a) *Access.* Reviewing or obtaining copies by individuals of their own records that are part of a system of records.

(b) *Agency.* For purposes of disclosing records subject to § 806b.15, the Department of Defense is an agency as defined by the Privacy Act. For all other purposes, including applications for access and amendment, appeals from denials, exempting systems of records, etc., the Department of the Air Force is an agency.

(c) *Confidential source.* Any individual or organization that has given information to the Federal Government under:

(1) An express promise that the identity of the source would be withheld, or

(2) An implied promise to withhold the identity of the source made before September 27, 1975.

(d) *Confidentiality.* An explicit promise to withhold the identity of a source. For a promise of confidentiality to be effective, the information furnished must be put into a system of records that is authorized for an exemption under the Privacy Act and for which the Secretary of the Air Force has claimed an exemption.

(e) *Disclosure.* Giving information about an individual, by any means, to an organization or to an individual who is not the subject of the record. In the context of the Privacy Act and this part, this term only applies to personal information that is part of a system of records.

(f) *Individual.* A living citizen of the United States or an alien admitted for permanent residence. The Privacy Act rights of an individual may be exercised by the legal guardian of an incompetent, or by the parent of a minor.

Note.—The Privacy Act confers no rights on deceased persons, nor may their next of kin exercise any rights for them.

(g) *Maintain.* Includes "hold," "collect," "use," "control," or "disseminate."

(h) *Minor.* Any individual under the age of majority as determined by state law that governs the location of the facility where the records are kept. If there is no prevailing state law (for example, overseas), a minor is any individual under 18 years of age.

(i) *Official Use.* Any action by a member or employee of the Department of Defense which is prescribed or authorized by a regulation, and is intended to complete a mission or function of the department.

(j) *Personal Information.* Any item of information about a person that is not a matter of public record and is usually considered to be personal to the individual. It includes, for example, information about the individual's financial, family, social, and recreational affairs; his or her medical, educational (except military training), employment, political, or criminal history; or information that identifies, describes, or gives a basis for inferring personal characteristics, such as voice or fingerprints.

(k) *Privacy Act Request.* A request from an individual for information about the existence of, or for access to or amendment of, a record about him or her that is in a system of records. The request must cite or indicate a knowledge of the existence of the Privacy Act of 1974.

(l) *Record.* Any item, collection, or grouping of information about an

individual that is kept by the Government.

(m) *Routine Use.* Any use or disclosure of information from a system of records that has been listed in a published systems notice and that is consistent with the purpose for which the information was collected.

(n) *System Manager.* The official responsible for the policies and procedures for operating a system of records. The local systems manager operates and has immediate contact with the system.

(o) *Statistical Record.* A record kept for statistical or reporting purposes which is not used by making judgments about individuals. The identity of specific persons must not be discoverable using usual statistical or data manipulation methods.

(p) *System of Records.* Any group of records from which personal information is retrieved by the name of an individual or by some personal identifier, such as the individual's Social Security Number (SSN). If such retrieval is possible but not actually done, the group does not constitute a system of records. Likewise, if retrieval depends on the operator's memory, no system of records exists. However, the creation of a retrieval index, arranged by personal identifier for a system that is filed at random, makes that system a system of records. Notices for all systems must be published in the *Federal Register* and no system may be operated or maintained until this is done.

(q) *Workday or Day.* An official duty day, not including Saturdays, Sundays, and official Federal holidays.

§ 806b.3 Air Force supplements.

Commands will not change, through supplements or other publications, the policies and procedures set by this part. Send copies of each major command (MAJCOM) or separate operating agency (SOA) publication that implements this part to HQ USAF/DAAD(S), Wash DC 20330.

§ 806b.4 Responsibilities assigned.

(a) The Administrative Assistant to the Secretary of the Air Force (SAF/AA) has overall responsibility for the Privacy Act within the Air Force and is the final decision authority on all appeals.

(b) The Director of Administration, HQ USAF, manages and administers the program through the Air Force Privacy Act Office, HQ USAF/DAAD(S).

(c) HQ USAF Deputy Chiefs of Staff (DCS) (and comparable officials) and SAF offices make sure that their deputes or offices comply with this part and name a Privacy Act Officer to

assume the responsibilities in (g) of this subparagraph.

(d) MAJCOM and SOA Commanders implement this part within their commands and ensure compliance with its requirements.

(e) MAJCOM and SOA Directors of Administration monitor and administer the command-wide program. They may give these responsibilities to another staff function, if HQ USAF/DA approves. They name a command Privacy Act Officer within the Documentation staff function, and a Privacy Officer at each installation or tenant unit. They send the name, grade or rank, and telephone number of the current command Privacy Act Officer to HQ USAF/DAAD(S). Privacy Act monitors may be appointed at subordinate organizations and staff elements, if required.

(f) Command Privacy Act Officers:

(1) Serve as the primary point of contact within the command on all Privacy Act matters.

(2) Make sure that appropriate command personnel are trained or oriented in the provisions of the Act.

(3) Develop the command supplement to this part, if required.

(4) Gather material for the annual report and record system notices for HQ USAF/DAAD(S).

(g) Local Privacy Officers:

(1) Act as liaison between the command Privacy Act Officer and individuals who are responsible for operating systems of records.

(2) Implement, administer, and monitor the Privacy Act program within their areas of jurisdiction.

(3) Make sure that personnel are trained or oriented in the provisions of the Act.

(4) Compile material for the annual report, and records system notices for the command Privacy Act Officer.

(h) Record system managers may serve at any level in the Air Force. They determine the content and set rules for operating the system. System managers are responsible for sending public notices for proposed new or changed systems of records to the local Privacy Officer and for evaluating the systems each year, as required by § 806b.13. In many cases, record system managers also operate the system as the local system manager.

(i) Local records system managers or custodians answer requests for information from individuals, keep accountability records of disclosures, and send the Privacy Officer data needed for the annual report.

§ 806b.5 Delegation of authority.

(a) *Access authorities.* (1) The person named or position listed in the record system notice published in the Federal Register, either as the one to whom the request is to be sent or as the system manager.

(2) Reports of the Air Force Office of Special Investigations (AFOSI) released under rules in Part 952. Reports on investigations that are not complete and on which no final action has been made, are released by the commander of the organization that requests the investigation. Reports on completed investigations may only be released by HQ AFOSI.

(3) Inspector General complaint records, released only with the approval of HQ AFISC/IC.

(b) *Denial authorities.* The authority to deny access to, or to refuse to amend records must not be delegated to levels lower than those shown below, unless approved by SAF/AA. Send requests for waiver, with justification, to HQ USAF/DAAD(S), Wash DC 20330. Only the following officials, or their designees, have the authority to refuse to release or amend records:

(1) At SAF or HQ USAF, Deputy Chiefs of Staff and chiefs of comparable offices or higher level.

(2) At MAJCOM or SOAs, Commanders.

(3) For personnel records on civilian employees, Chief, Office of Civilian Personnel Operations (OCPO/MPK), Randolph AFB, TX 78148.

(4) For OSI investigative records, Commander, AFOSI, HQ AFOSI, Wash DC 20314.

Note.—The officials named above may designate one alternate denial authority. Send a copy of the letter of appointment to HQ USAF/DAAD(S), Wash DC 20330.

(c) *Authority to request law enforcement records.* The Commander, AFOSI; the Chief, Air Force Office of Security Police; Base Chiefs of Security Police; and AFOSI District Commanders and their designees are authorized to ask for records from any source for law enforcement activities under 5 U.S.C. 552a(b)(7). These requests must be in writing and indicate the particular part of the record desired and the law enforcement activity that is asking for the record.

§ 806b.6 Judicial sanctions.

The Privacy Act has both civil remedies and criminal penalties for violations of its provisions.

(a) *Civil remedies.* An individual may file a civil suit against the Air Force, if

Air Force personnel fail to comply with the Privacy Act.

(b) *Criminal penalties.* A member or employee of the Air Force may be found guilty of a misdemeanor and fined not more than \$5,000 for willfully:

(1) Maintaining a system of records without first meeting the public notice requirements. (See § 806b.12.)

(2) Disclosing individually identifiable information to one not entitled to have it.

(3) Asking for and getting another's record under false pretenses.

Subpart B—Collecting Personal Information**§ 806b.7 Collecting from the individual.**

Collect personal information, as much as possible, directly from the individual. Do not collect this information from third parties unless:

(a) The accuracy of information supplied by an individual must be verified with a third party.

(b) The information can only be obtained from a third party, such as information about how an employee performed in an earlier job or assignment.

(c) Getting the information from the individual would present exceptional difficulties or would result in an unreasonable cost.

(d) Other compelling and unusual circumstances make third party involvement necessary.

§ 806b.8 Privacy Act statements.

If the information asked for would be releasable under the FOIA, there is no requirement to give the person a Privacy Act Statement (some examples of this kind of information are name, grade, organization, duty assignment, and official telephone number). In all other cases, give individuals who are asked for information about themselves a Privacy Act Statement. This must be done regardless of how you collect or record the information, whether you use a form in the usual sense (that is, a printed document with a control number and edition date) or a blank page. You may advise individuals orally or display a sign in areas where they are frequently required to supply the same type of information; however, printed copies must be available and given to the individual on request. A Privacy Act Statement, whether given orally or placed on a form, must include:

(a) The number of the statute or executive order that authorizes collecting the information.

(b) The principal purposes for which the information will be used (for

example, why the information is requested).

(c) The routine uses to be made of the information (for example, how the information is going to be used).

(d) Whether furnishing the information is mandatory or voluntary. Responding is mandatory, only if the information is essential to the Air Force mission, and if failure to furnish it could make the person liable to some administrative or disciplinary action.

(e) What will happen to the individual, if he or she does not give all or any part of the information requested.

Note.—If you ask an individual for his or her SSN, you must state whether disclosure is voluntary or mandatory, give the statute or authority for requesting it, and state how it will be used.

(1) An individual may not be denied any right, benefit, or privilege provided by law for refusing to give his or her SSN unless disclosure:

(i) Is required by Federal statutes; or
(ii) Was required under statute or regulation adopted before January 1, 1975 for a system of records operating before that date.

Note.—Executive Order 9397, November 22, 1943, authorizes the use of the SSN as a system of numerical identification of individuals.

(2) The fact that disclosure of the SSN is not required by Federal statute or is not for a system of records operating before January 1, 1975, does not preclude Air Force officials from asking for it. However, the Privacy Act Statement must make clear that disclosure of the SSN is voluntary. If the individual refuses to disclose it, be prepared to use other means for identification.

Note.—The Forms Management office provides information on preparing and processing forms that should have Privacy Act Statements. The Publications Management office ensures that a Privacy Act warning statement is in the preamble of each regulation that calls for collecting personal information.

§ 806b.9 Promises of confidentiality when collecting information about individuals from third parties.

Give these promises rarely, and only for information that could not be obtained by other means. These promises can only be given for information that is put in an exempt system of records (see Subpart E). In order to exempt information under subsections (k)(2), (k)(5), and (k)(7) of the Privacy Act, sources must be given an express promise that their identities will not be revealed.

Subpart C—Maintaining Information in Systems of Records

§ 806b.10 Air Force standards.

The Air Force must maintain information on individuals with such accuracy, relevancy, timeliness, and completeness as is reasonably necessary to make sure that determinations about them are made fairly.

(a) No record in a system of records will be kept unless it is authorized by statute or by Executive Order and is directed by an Air Force regulation.

(b) No record in a system of records will be kept unless it is relevant and necessary to carry out the mission or a function of the Air Force.

(c) No record will be kept that describes how an individual exercises any right guaranteed by the First Amendment to the Constitution unless expressly authorized by statute, by the individual concerned, or unless authorized for a law enforcement purpose.

(d) No system of records or revised system of records will be operated until the requirements for public notice and report to the Office of Management and Budget have been met. (See § 806b.12.)

(e) An activity must not issue a Request for Proposal or an Invitation to Bid for computer or communications systems and services to support a new or altered system of records until the requirement for a report to the Office of Management and Budget has been met. (See § 806b.12.)

(f) No record from a system of records will be released except according to Subpart D.

§ 806b.11 Protecting records.

Any activity that operates a system of records must set rules of conduct, operating procedures, and physical safeguards to keep the records safe from unauthorized disclosure. The level of protection should be in line with the level of sensitivity of the information.

(a) *Disposition of Records.* Dispose of records that have personal data and are eligible for disposal (as directed by AFM 12-50, Disposition of Air Force Documentation) by tearing into pieces, shredding, pulping, macerating, or burning.

(1) Dispose of magnetic tapes or other magnetic medium by degaussing or erasing.

(2) Activities may dispose of computer cards and printouts in a volume of 5 cubic feet or more without removing information subject to the Privacy Act from the records. This amount is sufficient to make sure that any one item

of information becomes lost in the accumulated whole. It is not a disclosure under the Privacy Act. The carbon paper associated with these products may be disposed of through normal waste disposal methods. Systems managers may ask for a waiver of the required volume from command Privacy Act Officers. Systems Managers must give substantial reasons to justify any reduction. Command Privacy Act Officers review the request in consultation with the Staff Judge Advocate. If there is disagreement, the request may be sent to HQ USAF/DAAD(S) for a final determination.

(b) *Safeguarding personal information in ADP Systems.* See AFR 300-13, Safeguarding Personal Data in Automatic Data Processing Systems.

§ 806b.12 Public notice and reporting requirements.

The Privacy Act requires that a report on all new or altered systems of records be published for public inspection. In addition, the Office of Management and Budget (OMB) requires a report on new systems and certain kinds of altered systems. Instructions on how to prepare both the OMB report and the systems notice are in § 806b.21. New systems notices, changes to current systems notices, and the OMB report, if required, must reach HQ USAF/DAAD(S), Wash DC 20330 at least 90 days before the date an activity will begin to operate a new system, change an existing system, issue any data collection forms or instructions, or issue a request for proposal or invitation to bid for computer or communications systems or services to support the new or altered systems.

(a) A new system of records is one for which no notice has been published in the **Federal Register**. It requires both a systems notice and an OMB report.

(b) An altered system of records, requiring both an OMB report and a systems notice, is one that:

(1) Significantly increases the number or changes the types of individuals on whom records are kept.

(2) Expands the categories of information. For example, a system that has physical training records is expanded to include medical records.

(3) Alters the way in which records are organized or in which they are indexed or retrieved so as to change the nature or scope of the records. For example, combining two or more existing systems as a result of centralizing a unit's responsibilities is an alteration.

(4) Alters the purpose for which the information is used.

(5) Alters the computer environment (for example, equipment configuration, software, or procedures) so as to create the possibility for greater or easier access (for example, adding a remote terminal at an office that did not previously have access to a system).

(c) An altered system of records that requires an amended systems notice but not an OMB report, is one that:

(1) Alters or adds routine uses within the scope of the original purpose for which the information was collected.

(2) Decreases the number of persons on whom records are kept.

(3) Adds a new data element clearly within the scope of the existing categories, or decreases the number of categories.

(d) A systems manager who decides a system of records must be exempted from some or all of the requirements of the Privacy Act must send a letter through the command Privacy Act officer to HQ USAF/DAAD(S) Wash DC 20330, giving specific reasons. This request must be processed by the Air Force Privacy Act Office for Secretarial approval (See Subpart F).

§ 806b.13 Evaluating systems of records.

Each system manager must evaluate the system of records and each category of information in the system at least once a year to make sure they are still relevant and necessary. Send any amendments or deletions as prescribed in § 806b.12. Take into consideration:

(a) How the system and each item of information in it relate to the program it supports and to the statutory purpose of the program.

(b) What the specific adverse consequences of dropping the system or any item of information in it would be.

(c) The possibility of meeting information requirements by using other than personal data.

(d) The possibility of early purging of any item of information.

(e) The cost of running the system as it is, in relation to the result of discontinuing it.

Subpart D—Disclosing Information From Systems of Records

§ 806b.14 Disclosures to the subjects of records.

Individuals may ask whether the Air Force is maintaining records about them. If such records exist within systems of records, the Privacy Act gives the individual a right of access to the record, and a right to request its amendment.

(a) *How to identify a Privacy Act request.* To be considered under the Privacy Act, a request must:

(1) Come from a person whose records are in the system, or who is a designated agent or legal guardian. The request can be either oral or written.

(2) Cite the Privacy Act or at least show an awareness of the Act's requirements. For example, it could be addressed to the Privacy Act Officer, system manager, or FOIA manager, even if it does not cite the Act in the text of the request. Because people sometimes confuse the Privacy Act and FOIA, a request that cites or implies FOIA will be treated as a Privacy Act request, if it meets all the other criteria in this section.

(3) Pertain to records that are in a system of records. If the records the person wants are not in a system of records, the request falls into a category other than Privacy. The request does not have to name the system, but it should be fairly specific. Do not accept blanket requests for "all records about me." Instead, refer the person to AFP 12-37, Access Guide for Making Freedom of Information Act and Privacy Act Requests, and ask for more details.

(b) *How to identify a functional request.* Other Air Force directives give individuals the right to have access to their records. If an individual asks for his or her records and does not cite, or reasonably imply, the Privacy Act or FOIA, and another prescribing directive authorizes the release of the records, use that directive as authority for the release. Apply the schedule of fees in Part 813. Do not count the request as a Privacy Act request. An example is when an officer asks a personnel clerk for a copy of his or her Officer Effectiveness Report (OER). If the officer does not cite Privacy Act or FOIA, the clerk may give him or her the record under AFR 36-10, Officer Evaluations, and charge according to Part 813.

(c) *How to process a Privacy Act request for existence or access that cites Privacy Act, FOIA, or both.* Regardless of whether a person cites or implies the Privacy Act or the FOIA, process the request so as to give the most information possible. This may mean processing part of the request under one Act and part under another.

(1) *Verifying identity.* When local systems managers receive a request for information about the existence of, or for access to, records, they must verify the requester's identity, unless the record sought is available to anyone under the FOIA. The person does not have to state a reason for the request, nor can the request be denied, if the

person does not give his or her SSN, unless disclosure of the SSN is required by Federal Statute or by a regulation adopted before January 1, 1975.

(2) *Notify the requester.* Once the requester's identity is assured, the local system manager or custodian should:

(i) Within 10 working days from the date the request was received, tell the person if the system of records has a record about him or her, and when and where it may be reviewed.

(ii) Within 30 working days from the date the request was received, let the person review the record, or obtain a copy, unless it is exempt and listed in § 806b.22.

(a) If the requester wants to bring another person, the local manager may ask for written authorization for the other person to be present during any discussion of the content of the record.

(b) There is no requirement to create a record to fulfill a request; the record must be in existence at the time of the request. However, do not deny a record just because it is not readily available in a convenient format. Information in a system of records on magnetic or computer tape should be given in a format the requester can read.

(3) *Assessing fees.* When providing documents under the Privacy Act, charge fees for reproduction only.

(i) Use the following fee schedule:

Office copy (per page).....	.10
Microform media (paper copy) (per image).....	.25
Microfiche (per fiche).....	.95

(ii) Do not charge fees for:

(a) Performing record searches.

(b) Reproducing a document for the convenience of the Air Force.

(c) Reproducing a record only in order to let a requester review it. If he or she wants a personal copy, use the fee in (3)(i) of this subpart.

(d) Reproducing a record for a requester who shows that he or she cannot pay the allowable charge.

(iii) Waive the fee, if the total amount is less than \$5.

(4) *Denying access.* If the local systems manager decides the record should not be released, he or she sends a copy of the request, a copy of the record (or records), and the reasons for recommending denial, including the exemption being applied, to the Denial Authority, through the command Privacy Act Officer. This must be done within 5 workdays from the date the request was received.

(i) *Evaluation of record.* No record may be withheld just because it is in an exempt system. Before recommending denial, the local manager must:

(a) Make sure the system is covered by an exemption approved by the Secretary of the Air Force and listed in § 806b.22.

(b) Make sure that each document is, in fact, covered by the exemption, since all documents in a system are not automatically exempt.

(c) Determine that no part of the record could be released, either by careful editing or in the form of a summary. If a record has both releasable and exempt material, the releasable part must be separated and made available.

(ii) *Medical records.* If, in the judgment of a physician, releasing a medical record to the subject could harm the subject's mental or physical health, the system manager may require the requester to name a physician to receive the record. This is a denial of the record, only if the subject refuses to name a physician.

(iii) *Third party information.* A record with personal information about someone else can be released after the third party information has been taken out. If the information is releasable under the FOIA, it is not deleted. If the record is one to which the requester has already had access, such an order or effectiveness report, it is released intact. In all other cases, personal information such as home addresses and SSNs of others should be deleted. If there is information in the record, the disclosure of which would be a clearly unwarranted invasion of someone else's privacy, that information should be withheld.

(iv) *Information compiled for litigation.* Information in a system of records compiled in reasonable anticipation of a civil action or proceeding may be denied. The requester should be informed of his or her right to appeal this denial.

(v) *Denial Authority action.* (a) The Command Privacy Officer reviews the denial recommendation and consults with the servicing Staff Judge Advocate and the office responsible for the program under which the record was created. He or she makes a recommendation to the Denial Authority, consistent with the results of this review.

(b) The Denial Authority, after examining the case, notifies the requester whether or not access will be granted. If the Denial Authority decides to grant access, he or she instructs the local systems manager to release the record. If the Denial Authority denies access, he or she must tell the requester why, and that the decision may be appealed to the Secretary of the Air

Force within 45 days after the denial letter is received. The requester will be told to resubmit the original request and send any supporting material back to the Denial Authority for forwarding to HQ USAF/DA, Wash DC 20330. The requester should be cautioned that failure to follow this procedure may delay the appeal.

(d) *How to process a request for amendment.* Individuals may ask the Air Force to amend records about them that are in a system of records. The amendment sought must change, delete, or add material to make a record factually accurate, timely, relevant, or complete. A request that asks for an amendment of information that is subjective, or involves a matter of opinion or interpretation, is not processed under this part. It is sent back, and the person told to send it to the Air Force Board for the Correction of Military Records under Part 865, Subpart A of this chapter, under grievance procedures in AFR 40-771, Appeal and Grievance Procedures, or any other appropriate directive.

(1) Requests to amend may be made orally or in writing. But, only requests asking for minor corrections are accepted orally. In either case, the local systems manager verifies the identity of the person seeking the amendment.

(2) Local systems managers routinely correct any record, if the requester can conclusively show it is factually in error, or if no lawful purpose would be served by not correcting the record. In these cases, the manager makes the change, notifies all holders of the record, and informs the individual when the correction is made.

(3) If the manager decides not to amend the record, he or she sends a copy of the record, the reasons for denial, and the request to the Denial Authority through the command Privacy Act Officer. The Command Privacy Act Officer reviews the denial recommendation and consults with the servicing Staff Judge Advocate and the office responsible for the program under which the record was created. He or she makes a recommendation to the Denial Authority based on the results of this review. A Denial Authority who decides to support, or partially support denial, sends the requester a letter stating why the request was denied and how to appeal the decision. If a review does not support denial, the system manager must be told to amend the record and notify all subsequent recipients of the change.

TABLE 1

PRIVACY ACT REQUEST PROCESSING

R U L E	A	B	C	D
	If requester cites or implies (see note 1)	and asks for	which are	then process as a
1	Freedom of Information Act (FOIA)	his or her own records	in a system of records	Privacy Act (PA) request under AFR 12-35 (see note 2).
			not in a system of records	FOIA request under AFR 12-30.
		someone else's records	filed anywhere	
2	Privacy Act (PA)	his or her records	in a system of records	PA request under AFR 12-35 (see note 2).
			not in a system of records	FOIA request under AFR 12-30.
		someone else's records	filed anywhere	
3	neither Act	his or her own records	in a system of records	Functional request. If a regulation provides access, use its procedures. Otherwise, use AFR 12-35.
			not in a system of records	Functional request. If a regulation gives access use its procedures. If the functional regulation would deny access, see AFR 12-30.
		someone else's records	filed anywhere	
4	both acts	his or her own record	in a system of records	PA request under AFR 12-35 (see note 2) or FOIA request under AFR 12-30 or both, whichever gives most information.
			not in a system of records	
		someone else's record	filed anywhere	FOIA request under AFR 12-30.

NOTES: 1. Request for information from subject of an AFOSI investigation should be processed under AFR 12-30.

2. Report as Privacy Act Request in Annual Report.

BILLING CODE 3910-01-C

(e) *Time limits.* Requesters should be told what action will be taken on their request within 10 workdays from the date the first Air Force office receives it. If access is granted or a record is amended, that should usually be done within 30 workdays. Table 2 gives time limits for the persons responsible for these actions. If the 10-day time limit

cannot be met, the requester should be sent a letter telling why a delay is needed and giving an approximate response date. That date should be no more than 20 workdays after the first Air Force office receives the request. Send a copy of this letter to HQ USAF/DAAD(S), Wash DC 20330, through Privacy Act channels.

TABLE 2

TIME LIMITS FOR PROCESSING PRIVACY ACT REQUESTS

R U L E	A	B	C
	If you	and you are	then the time limit is
1	transfer action to another systems manager	Any recipient	2 workdays from receipt.
2	transfer action to Denial Authority	local Systems manager	5 workdays from receipt.
3	acknowledge request and tell requester if record exists		10 workdays*.
4	acknowledge request and tell requester access will be granted	local Systems Manager, or Denial Authority	10 workdays*.
5	acknowledge request and tell requester amendment will be made		
6	Tell requester that access is denied	Denial Authority	
7	tell requester that amendment is denied		
8	grant access or amend record	local System Manager	30 workdays*.

NOTE: Time limits for granting access are recommended only; *From initial receipt by an Air Force activity. time limits for amending are required by the Privacy Act.

(f) *Appeals of initial refusals to grant access or to amend records.* (1) *Request for secretarial review.* An individual may request a review of the initial refusal by writing to the Secretary of the Air Force within 45 days of the denial. The request should be addressed to the Secretary of the Air Force (SAF/AA), Wash DC 20330 and sent back to the initial Denial Authority for forwarding to HQ USAF/DA, Wash DC 20330. The Denial Authority sends a complete file in the following order:

- (i) The request for review.
- (ii) The initial request for access or amendment.
- (iii) The initial refusal.
- (iv) A copy of the record or portions involved.

(v) Any internal records or coordination actions that relate to the initial refusals.

(vi) Denial Authority comments on the appellant's arguments.

(2) *Responsibilities for Review.* (i) The Air Force Privacy Board reviews the initial denial and makes recommendations to the Vice Chief of Staff (CV). Members of the Board are representatives from HQ USAF/DA (Chairperson), the Office of The Judge

Advocate General (HQ USAF/JA), and an Air Staff function not having primary responsibility for the record in question. The Chairperson may also call upon subject matter experts to advise the Board. CV may designate another official to serve as chairperson or, if the record is the primary responsibility of HQ USAF/DA or HQ USAF/JA, may choose a member from another Air Staff organization to sit on the Board instead.

(ii) The Office of the CV considers the recommendations of the Board and decides whether to direct the initial Denial Authority to grant access to or amend the record, or to uphold the denial. If the decision is to uphold, this recommendation is passed to SAF/AA through SAF/GC for a final decision.

(iii) SAF/AA considers HQ USAF/CV recommendations to uphold a denial, decides to grant or deny the appeal, and notifies both the individual and the initial Denial Authority of the decision. If SAF/AA upholds the denial, the individual is advised of his or her right to send a statement of disagreement to the system manager.

(3) *Time limits for appeal.* Table 3 shows the necessary actions and time limits for each part of the appeal process.

TABLE 3

APPEAL PROCESSING

R U L E	A	B	C	D
	If	Decides to	then	within
1	AF Privacy Board	uphold denial OR overrule denial of access OR overrule denial of amendment	Pass to HQ USAF/CV with recommendations	15 work days.*
2	HQ USAF/CV	uphold denial	pass to SAF/AA through SAF/GC with recommendations	30 work days*.
		overrule denial of access OR overrule denial of amendment	Notify the Individual and instruct Denial Authority to have access granted or record amended	
3	SAF/AA	uphold denial of access	notify the individual, giving reasons with copy to Denial Authority	45 work days*.
		uphold denial of amendment	Notify individual giving reasons. Invite individual to file statement of disagreement with systems manager stating any reasons for disagreeing with the Air Force's decision. Tell individual that statement will become permanent part of record, shown to all subsequent users and sent to prior recipients.	
		overrule denial of access	Notify individual. Instruct Denial Authority to have access granted or record amended	
4	overrule denial of amendment			

*Time from receipt of appeal by HQ USAF/DA.

(g) *Statements of disagreement.* If an individual submits a statement of disagreement with the Secretary of the Air Force's decision not to amend his or her record, the local system manager:

(1) Flags the record so that the disagreement may be seen by anyone who discloses or gains access to the record.

(2) Files the statement with the record. If this is not possible, maintain it to allow ready retrieval when the disputed portion of the record is used.

(3) Advises previous recipients that the record has been disputed and gives

them a copy of the disagreement statement, if they can be identified.

(4) Lets subsequent users know that the record is disputed and gives them a copy of the statement along with the record. The manager may include a brief summary of the reasons for not amending the record. Summaries are limited to the reasons SAF/AA gives to the individual. The summary is treated as a part of the individual's record, but is not subject to the amendment procedures.

(h) *Privacy Act case files.* Except for the statement of disagreement, do not file documents used in processing notification, access and amendment

requests (including appeals) in or with the system of records to which they pertain. Instead, set up Privacy Act case files. These files should include requests from, and replies to, individuals on whether a system has a record about them; requests for access, approvals, refusals, appeals, and final review action; and coordination actions and related papers. Do not keep a copy of the disputed record in the case file. Use the file solely to process requests and as a source of statistics. Do not use it as a source of precedents for processing similar actions. Do not use it to make any other kind of determination about the individual. Set up Privacy Act case files at each office that processes a request.

§ 806b.15 Disclosures to third parties and organizations.

The fact that the Air Force lets an individual know why we are collecting the information and how it will be used does not mean we have his or her consent to release it. Thus, when we decide to release information as authorized below, we must first consider all the consequences of that disclosure. Before we release any information, we must make a reasonable effort to ensure that it is accurate.

(a) *With subject's consent.* Unless prohibited by other statutes or directives, we may disclose information from a system of records if the subject of the record writes and asks us to, or if he or she has given prior written consent by signing a release form. For example, medical information could be released to an insurance firm with the subject's written authorization. Make sure, however, that there is no statute or directive that prohibits release. For example, drug or alcohol abuse treatment information kept in connection with a drug or alcohol prevention function may be released only as authorized by 21 U.S.C. 1175 and 42 U.S.C. 4582. For this information to be released, the subject's specific consent is needed; general consent is not enough.

(b) *Without subject's consent.* A person's records may be disclosed without his or her consent to:

(1) Department of Defense officials and employees who need the record to perform their duties and who use it for the purpose for which we collected it.

(2) The public, as required by the FOIA. See Part 806 of this chapter.

(i) Some examples of information that can be released for military personnel without an unwarranted invasion of privacy are: name; rank; date of birth; marital status; name, age, number and

sex of dependents; date of rank; gross pay; present and past duty assignments and future assignments which are firm; office and unit address and phone number; source of commission; military and civilian education level, including major area of study, school, year of graduation and degree; promotion sequence number; awards and decorations; duty status at any given time; official photograph; and home of record, without street address. See Federal Personnel Manual Supplement 990-1, Part 294, on release of civilian personnel information.

(ii) Disclosing a person's home address, SSN, or home telephone number without his or her consent is usually considered to be a clearly unwarranted invasion of privacy. Thus, disclosure under FOIA usually should not be made.

(iii) Apply a balancing test to decide whether disclosure would be a clearly unwarranted invasion of the individual's privacy. Weigh the individual's right to privacy versus the public's right to know. Consider the nature of the information to be disclosed; do individuals usually expect this information to be kept private? Are the identities of the subject and the recipient already in the public eye? What is likely to happen to the individual as a result of the disclosure? How old is the information; is it still relevant? To what degree is the information already in the public domain?

(iv) We may release information, if the balancing test described above weighs in favor of disclosure. For example, we may be permitted to disclose home addresses to a requester who wanted to enforce a court order for alimony or child support payments, or to local and state tax authorities to enforce tax laws.

(v) We may not sell or rent lists with individuals' names and home addresses. Likewise we may not, without individuals' consent, release lists of names and home addresses to the public. We must allow individuals to decide if they want their home addresses and phone numbers included in base directories.

(3) Agencies outside the Department of Defense for a routine use which has been listed in the systems notice describing the system of records and has been published in the *Federal Register*. The routine use must be compatible with the purpose for which the information was collected and must be within the expectations of the person when he or she furnished it.

(4) The Bureau of the Census to plan or carry out a census or survey under Title 13, U.S.C.

(5) A recipient for statistical research or reporting. The recipient must give us advance written assurance that the record will be used solely as a statistical research or reporting record. The record must not be used, in whole or part, to make any decisions about the individual's rights, benefits, or entitlements. It must be sent in a form in which the identity of the individual cannot be found out through usual research methods.

(6) The National Archives of the United States has a record with enough value to warrant keeping it, or for evaluation by the Administrator of the General Services Administration to see if the record has such value. However, when we send records to Federal Records Centers for storage, they stay under Air Force control. These transfers are not disclosures under this subpart and do not need an accounting.

(7) An agency outside the Department of Defense for a civil or criminal law enforcement activity authorized by law. The head of the agency or a designee must send a written request to the systems manager. The request must specify the record or part needed and the law enforcement purpose for which it is wanted. A record may also be disclosed to a law enforcement agency by the Air Force office that has it if criminal conduct is suspected. This disclosure is a routine use for all US Air Force records systems and has been published in the *Federal Register*.

(8) Another person or agency under compelling circumstances affecting the health or safety of an individual. The individual whose records are disclosed does not have to be the one in danger. For example, records on several persons could be disclosed to identify individuals injured in an accident. When individual records are disclosed in this way, we must send the subject a notification at the last known address.

(9) Either House of Congress, a congressional committee or subcommittee, for matters within their jurisdictions.

(10) A congressional office acting for a constituent who is the record subject. This disclosure is allowed by a blanket routine use.

(11) The Comptroller General or any authorized representatives on business of the General Accounting Office.

(12) A court of competent jurisdiction that has ordered us to do so. When a record is disclosed under compulsory legal process and the court makes public the fact that it has issued an order or

subpoena for the record, we must make reasonable efforts to notify the individual by mailing a disclosure statement to his or her last known address.

(13) A contractor who is operating a system of records under a contract to perform an Air Force function, such as personnel, payroll, or health systems management. In this case, the contractor is considered an employee of the Air Force and the system of records is considered an Air Force system. Disclosure of records to the contractor does not need the subject's consent nor does it require that an accounting be kept.

(c) Accounting for disclosures.

(1) For those disclosures for which an accounting is required, each local record system manager must keep an accurate record showing the date of the release, the specific information released, the basis for making the disclosure, and the name and address of the recipient (see table 4). Accounting is required, even if the subject gives written consent. Systems managers may file the disclosure accounting record in any way they want, as long as they can reconstruct it to:

- (i) Give to the subject on request.
- (ii) Pass corrected or disputed information in the record to previous recipients.
- (iii) Provide a cross-reference to show the basis for making the disclosure.
- (iv) Provide an audit trail for reviews of Air Force compliance with the conditions of disclosure outlined in this subpart.

(2) For some systems of records, subsections (j)(2) and (k) of the Privacy Act permit withholding the accounting record from the subject. § 806b.22 lists those systems. Also, an accounting of disclosures that were made for law enforcement purposes may be withheld.

(3) Dispose of the accounting record according to AFM 12-50.

TABLE 4

DISCLOSURE ACCOUNTING AND CONSENT REQUIREMENTS

R U L E	A	B	C	D	
	If information from a system of records is disclosed to	and pertains to	then it is under the	and requires	
				an accounting	written consent
1	an individual	the individual	Privacy Act (note 1)	No	No
2	any DOD activity	info for official uses	Privacy Act	Yes	No (note 2)
3	any person or organization outside of DOD other than the subject	a published Routine Use in the Systems Notice			
4	anyone but the subject outside DOD	emergencies affecting health or safety			
5	The Congress	official uses			
6	Bureau of the Census	census or survey or related activity			
7	The General Accounting Office	official uses			
8	The National Archives	info to be appraised or accepted for deposit			
9	A Court	an order of the court	FOIA	No	No (note 3)
10	anyone but the subject	info releasable under Freedom of Information Act (FOIA)			
11	any US agency or instrumentality	civil or criminal law enforcement	Privacy Act	Yes	

NOTES:

1. When a request cites neither PA or FOIA but another Air Force directive authorizes the release of the information, then the release is under that directive.

2. Notify the individual at his or her last known address.

3. Notify the individual as soon as the compulsory legal process becomes a matter of public record at his or her last known address.

BILLING CODE 3910-01-C

Subpart E—Exempting Systems of Records

The Secretary of the Air Force may exempt Air Force systems of records from certain parts of the Privacy Act. There are two kinds of exemptions: general and specific. The general

exemption relieves systems of records from most requirements of the Act; the specific exemption from only a few.

§ 806b.16 Exemption index and cross reference.

The index below shows for which

parts of the Privacy Act exemptions may be claimed. "No" means that no exemption may be taken; "yes" means that an exemption may be taken. Note that the index provides a cross reference to this part.

EXEMPTIONS		Privacy Act Section	AFR 12-35	
General 3(j)	Specific 3(k)		Paragraph	Page
no	no	3(b)(1-11): conditions of disclosure	15	
no	no	3(c)(1,2): making and keeping disclosure acctg	15	
yes	yes	3(c)(3): individual access to accounting	15	
yes	no	3(c)(4): informing prior recipients of corrections	14	
yes	yes	3(d)(1-5): access to records	14	
yes	yes	3(e)(1): restrictions on collection of info	1	
yes	no	3(e)(2,3): collecting from individual	7	
no	no	3(e)(4)(A-F): publishing systems notices	12	
yes	yes	3(e)(4)(G-I): system access & source descrpt.	12,14	
yes	no	3(e)(5): standards of accuracy	10	
no	no	3(e)(6,7): validate before disclosure/no records on 1st Amend ment rights	10,15	
yes	no	3(e)(8): notification of compulsory disclosure	15	
no	no	3(e)(9-11): rules of conduct/safeguards/routine use publication	1,11,12	
yes	yes	3(f)(1-5): agency rules	14	
yes	no	3(g)(1-5): civil remedies	6	
yes	no	3(h): rights of legal guardians	1	
no	no	3(i)(1-3): criminal penalties	6	
—	no	3(j)(1-2): general exemptions	17	
yes	—	3(k)(1-7): specific exemptions	18	
yes	no	3(l)(1-3): archival records	15	
yes	no	3(m): Government contractors	15	
yes	no	3(n): mailing lists	15	
yes	no	3(o): report on new systems	10	
yes	no	3(p): annual report	20	
no	no	7(a,b): restrictions on using SSN	8	

Figure 1. Exemption Index and Cross-Reference.

§ 806b.17 General exemptions.

Only US Air Force activities actually engaged in law enforcement may claim the general exemption for a system of records. These include the Staff Judge Advocate and correctional activities. This exemption appears in the Privacy Act in subparagraph (j)(2).

(a) To qualify for the exemption, a system must consist of:

(1) Data, compiled to identify individual criminals and alleged criminals, which consists only of identifying data and arrest records; type and disposition of charges; sentencing, confinement, and release records; and parole and probation status;

(2) Data that supports criminal investigations (including efforts to prevent, reduce, or control crime) and reports of informants and investigators that identify an individual; or

(3) Reports on a person, compiled at any stage of the process of law enforcement, from arrest or indictment through release from supervision.

(b) When we claim a general exemption for a system of records, the only parts of the Privacy Act we are required to comply with are subsections (b), (c) (1) and (2), (e)(4) (A) through (F), (e) (6), (7), (9), (10), and (11), and (i). See figure 1.

§ 806b.18 Specific exemptions.

(a) The Secretary of the Air Force has exempted a few systems of records that have the following kinds of information from certain parts of the Privacy Act. The Privacy Act exemption number appears in parentheses after each category below.

(1) Classified information in any Air Force system of records. Before denying a person access to classified information, the Denial Authority must make sure that it was properly classified under the criteria of Executive Order 11652 or 12065, and that it must remain so in the interest of national defense or foreign policy [(k)(1)].

(2) Investigatory data for law enforcement purposes (other than that claimed under the general exemption). But, if this information has been used to deny someone a right, we must release it unless doing so would reveal the identity of a confidential source [(k)(2)].

(3) Data kept to protect the President of the United States and others, as authorized by 18 U.S.C. 3056[(k)(3)].

(4) Statistical data required by statute and used only for statistical purposes and not to make decisions on the rights, benefits, or entitlements of persons [(k)(4)].

(5) Data compiled to determine suitability, eligibility, or qualifications for Federal service, Federal contracts, or

access to classified information. We may withhold this information, only if disclosure would reveal the identity of a confidential source [(k)(5)].

(6) Tests to find out whether to appoint or promote a person in the Federal Service. We may withhold this information, only if disclosure would compromise the objectivity or fairness of the examination process [(k)(6)].

(7) Information to determine promotion potential in the Armed Forces. We may withhold this information, only to the extent that disclosure would reveal the identity of a confidential source [(k)(7)].

(b) We do not have to comply with the following parts of the Privacy Act in operating a system for which we claim a specific exemption: subsections (c)(3); (d); (e)(1); (e)(4) (G), (H), and (I); and (f) (see figure 1).

Subpart F—Other Administrative Actions**§ 806b.19 Training.**

There are three kinds of training:

(a) *Orientation.* Command and local Privacy Officers must make sure that everyone in their areas of responsibility gets an initial orientation on how the Act works and what are the individual's rights and responsibilities under it. In addition, they must regularly conduct refresher training through Commanders Calls, articles in base bulletins, papers, and so forth.

(b) *Specialized.* This training takes place at USAF technical schools. It is for personnel who actually operate systems of records, or supervise their operation. Training elements that develop new blocks of instruction or alter old blocks must send them to HQ USAF/DAAD (S) for review.

(c) *Management.* Command and local Privacy Officers give commanders and their deputies management training that supplements the basic orientation. This training lets top managers know how the Act affects their operational decisions. For example, managers need to know that they will not be able to operate a system of records until 45 days after it has been published in the *Federal Register* for public comment. Also, this training gives Denial Authorities the information they need to act in this capacity.

§ 806b.20 Annual Privacy Act Report, RCS: DD-A (A & AR) 1379.

(a) Each Command Privacy Act Officer must report the following statistical information to the Air Force Privacy Act Office no later than March 1 of each year. The Report Control Symbol is DD-A (A & AR) 1379. The

report must cover the previous year's activity. Data should be given for each system of records. The data must include the number of:

(1) Requests for existence of records.

(2) Requests for access to records under the Act.

(3) Privacy Act requests returned for lack of sufficient information to identify the records.

(4) Requests for access totally granted and number partially granted.

(5) Requests for amendment of records under the Privacy Act.

(6) Requests for amendment totally granted and number partially granted.

(7) Exemptions used to deny access by citation number (j2, j5, k1-k7, and d5).

b. Each Privacy Act Officer should also keep a record of any unusual problems that arise in the course of the year about the administration of the Act. Report these in narrative form.

c. The Air Force Privacy Act Office provides statistical reporting forms and instructions no later than December 31 of each year.

§ 806b.21 Systems notice requirements.

Each system of records operated by the Air Force must be covered by a systems notice published in the *Federal Register*. You must send two copies of this notice, with a report of a new system, through the command Privacy Act Officer to HQ USAF/DADD (S) at least 90 days before operating the system. All items of information must be completed, and you should be as specific as possible. Use the following format:

How To Prepare Systems Notices and Reports

F01101 MAC ("F" indicates Air Force, the number is the table and rule from AFM 12-50 for records disposition, and the letters show the command or DCS)

System name: (Use a short, specific plain language title for the system)

System location: (Address of primary system and any decentralized elements; if system is Air Force-wide, show functional office)

Categories of individuals covered by the system: (List categories, but be specific; do not say all Air Force officers when the system applies only to officers of one command)

Categories of records in the system: (List specific elements of information; do not list form numbers)

Authority for maintaining the system: (Cite specific statute from the US Code or Executive Order that directs the program the records support; do not use Title 44)

Routine uses of records maintained in the system, including categories of users and the purposes of such uses: (Show the purpose of the system and all routine users who are not part of the Department of Defense (DOD). Give specific reasons for disclosure to agencies or persons outside of the DOD)

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage: (Show how records are stored listing the storage medium and types of containers)

Retrievability: (List all data elements used for retrieval)

Safeguards: (Provide a specific list of safeguards by categories such as guards, alarmed buildings, safes; do not describe any specific safeguards in a way that would jeopardize security)

Retention and disposal (Show length of retention from AFM 12-50 using the table and rule listed in the System Identification)

System manager(s) and address: (List the title and office address of the individual or individuals responsible for the system)

Notification procedure: (Give the title and address of any individuals who can tell people if their records are in the system)

Record Access procedure: (Tell who to contact for access giving title and address)

Contesting record procedure: (Leave blank)

Record source categories: (Show categories of individuals or other records used as sources for the system)

System exempted from certain provisions of the Act: ("None" unless you have filed an exemption, in which case list the sections of the Privacy Act from which the system is exempt)

(a) *Report of a new or altered system of records.* The report of a new or altered system must be sent through the Defense Privacy Board to the Congress and Office of Management and Budget by the Air Force Privacy Act Office. Systems managers must provide HQ USAF/DAAD(S), no later than 90 days before using the system or implementing the reportable change:

(1) System identification number and title of the system.

(2) Reason for creating the new system or for changing an existing system.

(3) A description of the change.

(4) The estimated number of individuals on whom records are kept in the system.

(5) Methods used to ensure accuracy of information in the system.

(6) A discussion of alternatives to using the system.

(7) The name, title, address and AUTOVON number of the person who knows how the system operates.

A complete system notice must be attached.

(b) *Nonreportable amendments or deletions.* Any change in the published systems notice that does not require a report to the Congress or to Office of Management and Budget must be sent at once to the Air Force Privacy Act Office. The following changes must be published in the Federal Register for public comment and must be sent at least 75 days in advance:

(1) Those that change the nature of or add to the routine uses of the system.

(2) Those that change the notification or access procedures.

§ 806b.22 General and specific exemptions claimed.

(a) *General exemption for criminal investigative files:* The Air Force claims the general exemption for the following systems of records: Counter Intelligence Operations and Collection Records, F12408 07YLNGA; Criminal Records, F12410 07YLNGA; Incident Investigation Files, F12501 SPO I; Investigative Support Records, F12404 07YLNGA.

(b) *Specific exemptions.* These are the systems for which we claim specific exemptions:

(1) *Classified records.* All records in systems of records that are properly classified per Executive Order 11652 or 12065, are exempt from 5 U.S.C. 552a (c)(3); (d); (e)(4) (G), (H), and (I); and (f), regardless of whether the entire system is otherwise exempt.

(2) *Air Force Academy Candidate System (F05302 OBXQPCB).* (i) *Exemption.* This system of records (Candidate Evaluation Record, Liaison Officer Evaluation, Letter of Evaluation from High School or College, and Drug Abuse Certificate) is exempted from 5 U.S.C. 552a (d), (e)(4)(H), and (f), but only to the extent that disclosure would reveal the identity of a confidential source.

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

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

(3) *Air Force Personnel Test 851, Test Answer Cards (F03506 DPMWA).* (i) *Exemption.* This system is exempt from 5 U.S.C. 552a (c)(3); (d); (e)(4) (G), (H), and (I); and (f).

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

(iii) *Reasons.* To protect the integrity of the promotion testing system by keeping the test questions and answers safe.

(4) *Cadet Personnel Record System (F03502 OBXQPCB).* (i) *Exemption.* Parts of this system are exempt from 5 U.S.C. 552a (d), (e)(4)(H), and (f), but only insofar as disclosure would reveal the identity of a confidential source.

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

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

(5) *Cadet Records (F04501 OKPNQSA).* (i) *Exemption.* Portions of this system (Detachment POC Selection Rating Sheets; AFOTC Form 0-24—

Disenrollment Review; Memoranda for Record and Staff Papers with Staff Advice, Opinions, or Suggestions) are exempt from 5 U.S.C. 552a (c)(3); (d); (e)(4) (G), and (H), and (f), but only to the extent that disclosure would reveal the identity of a confidential source.

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

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

(6) *Child Advocacy Case Files (F16802 SGPC A).* (i) *Exemption.* Parts of this system are exempt from 5 U.S.C. 552a(c) (3) and (d), but only to the extent that disclosure would reveal the identity of a confidential source.

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

(iii) *Reasons.* To encourage those who know of child abuse or neglect to come forward by protecting their identities. Also, to protect the integrity of on-going and civil law investigations of criminal and civil law violations. Giving subjects access to their files could result in them concealing, altering, or fabricating evidence, could hamper the identification of offenders and alleged offenders; and could jeopardize the safety and well-being of parents and their children.

(7) *Civilian Personnel Occupational and Suitability Employment Examinations (F04002 DPCMS D).* (i)

Exemption. Parts of this system are exempt from 5 U.S.C. 552a(c)(3); (d); (e)(4) (G), (H), and (I); and (f).

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

(iii) *Reasons.* To protect the confidentiality of a source who gives information about whether a person is qualified and suitable for civilian employment in the Federal service. Also, to protect test material used to determine qualifications so as to be fair to all candidates.

(8) *Class Committee Products (F01103XOBXQPCD).* (i) *Exemption.* Parts of this system are exempt from 5 U.S.C. 552a(d), (e)(4)(H), and (f), but only to the extent that they would reveal the identity of a confidential source.

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

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

(9) *Effectiveness/Performance Reporting Systems (F03501 DPMVO 1).* (i) *Exemption.* The parts of this system that have completed AF Forms 705,

Lieutenant Colonel Promotion Recommendation Report, and AF Forms 706, Colonel Promotion Recommendation Report, are exempt from 5 U.S.C. 552a(c)(3); (d); (e)(4) (G), (H), and (I); and (f), but only to the extent that disclosure would reveal the identity of a confidential source.

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

(iii) *Reasons.* To make sure that selection boards get candid evaluations of the potential of officers being considered for promotion to the grades of Colonel and Brigadier General.

(10) *Equal Opportunity in Off Base-Housing (F03005 PRENC A).* (i)

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

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

(iii) *Reasons.* To enforce civil laws, court orders, and the activities of the Departments of Housing and Urban Development and Justice.

(11) *General Officer Personnel Data System (F03501 AFDPG O).* (i)

Exemption. The parts of this system that have completed AF Forms 78, Air Force General Officer Effectiveness Report, are exempt from 5 U.S.C. 552a(c)(3); (d); (e)(4) (G), (H), and (I); and (f), but only to the extent that they would reveal the identity of a confidential source.

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

(iii) *Reasons.* To make sure selection boards get candid evaluations of the potential officers being considered for promotion to Major General, Lieutenant General and General.

(12) *Historical Airman Promotion Master Test File (F03508 DPMAM M).*

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

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

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

(13) *Inspector General Records*

(F12001 IGQ A). (i) *Exemption.* This system is exempt from 5 U.S.C. 552a(c)(3); (d); (e)(4) (G), (H), and (I); and (f). But, if a person is denied any right, privilege, or benefit he or she would otherwise be entitled to as a result of keeping this material, we must release the material unless doing so would reveal the identity of a confidential source.

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

(iii) *Reasons.* Granting individuals access to information collected while an Inspector General inquiry is in progress could interfere with the just, thorough, and timely resolution of the complaint or inquiry and could possibly enable individuals to conceal wrongdoing or

mislead the inquiring officer. Disclosure might also subject sources, witnesses, and their families to harassment or intimidation.

(14) *Investigative Applicant Processing Records (F12401 07YLNGB).*

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

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

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

(15) *Master Cadet Personnel Record (RR/Active) (F03502 OBXQPCE) and Master Cadet Personnel Record (RR/Historical) (F03502 OBXQPCD).* (i)

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

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

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

(16) *Military and Leadership Order of Merit System (F03001XOBXQPCB).* (i)

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

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

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

(17) *Personnel Files on General Officers and Colonels Assigned to General Officer Positions (F03501 AFREP T).* (i) *Exemption.* This system is

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

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

(iii) *Reasons.* To protect the integrity of information used in the Reserve Initial Brigadier General Screening Board, the release of which would compromise the selection process.

(18) *Personnel Security Case Files (F20503 DAI A).* (i) *Exemption.* This

system is exempt from 5 U.S.C. 552a(c)(3); (d); (e)(4) (G), (H), and (I); and (f), but only to the extent that disclosure

would reveal the identity of a confidential source.

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

(iii) *Reasons.* To protect the identity of those who give information in confidence for personnel security and related investigations. Fear of retaliation or exposure 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 fully develop or put to rest charges of questionable conduct. It is essential that all such allegations be resolved fairly and quickly.

(19) *Security and Related Investigative Records (F12406 07YLNGA).* (i) *Exemption.* This system

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

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

(iii) *Reasons.* To protect the identity of those who give information in confidence for personnel security and related investigations. Fear of retaliation or exposure 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 fully develop or put to rest charges of questionable conduct. It is essential that all such allegations be resolved fairly and quickly.

(20) *Special Security Files (F20505 SPIC).* (i) *Exemption.* This system is

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

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

(iii) *Reasons.* To protect the identity of those who give information in confidence for personnel security and related investigations. Fear of retaliation or exposure could cause them 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 fully develop or put to rest charges of questionable conduct. It is essential that all such allegations be resolved fairly and quickly.

Carol M. Rose,

Air Force Federal Register Liaison Officer.

[FR Doc. 79-11991 Filed 4-17-79; 8:45 am]

BILLING CODE 3910-01-M