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 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.

[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.[13]

(2) Public Law 100–235, The Computer Security Act of 1987,[14] which establishes minimum security practices for Federal computer systems.

(3) OMB Circular A–130, Management of Federal Information Resources,[15] 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,[16] December 13, 1999.

(7) DoD 5400.11–R, Department of Defense Privacy Program,[17] 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 consider 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,

[13] *http://www.defenselink.mil/privacy/1975OMB__PAGuide/jun1989.pdf.*

[14] *http://csrc.nist.gov/secplcy/csa__87.txt.*

[15] *http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html.*

[16] *http://www.dtic.mil/whs/directives/corres/html/540011.htm.*

[17] *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 (*http://www.foia.af.mil*).

Section D—Privacy Issues in Information Systems

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

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

Each agency that maintains a system of records shall:

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

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

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

Establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records

and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

Definitions

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

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

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

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

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

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

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

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

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

Information and Privacy

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

The use of information must be controlled.

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

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

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

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

Given the availability of vast amounts of stored information and the expanded capabilities of information systems to process the information, it is foreseeable that there will be increased requests to share that information. With the potential expanded uses of data in automated systems it is important to remember that information can only be used for the purpose for which it was collected unless other uses are specifically authorized or mandated by law. If the data is to be used for other purposes, then the public must be provided notice of those other uses. These procedures do not in themselves create any legal rights, but are intended to express the full and sincere commitment of the Air Force to protect individual privacy rights and which provide redress for violations of those rights.

DATA IN THE SYSTEM

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

Access to the Data

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

Attributes of the Data

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

Maintenance of Administrative Controls

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

(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.

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