

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Section B—Privacy and Systems Development

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

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

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

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

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

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

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

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

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

Section C—Completing a Privacy Impact Assessment

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

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

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

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

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

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

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