

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

Step	Who	Procedure
4 .....	MAJCOM Privacy Act Officer .....	Review the PIA document to identify privacy risks from the information provided. The MAJCOM Privacy Act Officer will get clarification from the owner and developer as needed.
5 .....	System Owner and Developer, MAJCOM Privacy Act Officer.	The System Owner, Developer and the MAJCOM Privacy Act Officer should reach agreement on design requirements to resolve all identified risks.
6 .....	System Owner, Developer, and MAJCOM 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 MAJCOM or HAF Functional CIO.
7 .....	MAJCOM or HAF Functional CIO .....	Issue final approval of PIA, and send a copy to AF-CIO/P for forwarding to DoD and OMB.
8 .....	AF-CIO/P .....	When feasible, publish PIA on FOIA Web page ( <a href="http://www.foia.af.mil">http://www.foia.af.mil</a> )

### Section D—Privacy Issues in Information Systems

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

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

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

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

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

Establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

#### *Definitions*

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

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

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

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

Record—any item, collection or grouping of information about an individual and

identifiable to that individual that is maintained by an agency.

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

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

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

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

#### *Information and Privacy*

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

The use of information must be controlled. Information may be used only for a necessary and lawful purpose.

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

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

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

Given the availability of vast amounts of stored information and the expanded capabilities of information systems to process the information, it is foreseeable that there will be increased requests to share that information. With the potential expanded uses of data in automated systems it is important to remember that information can only be used for the purpose for which it was collected unless other uses are specifically authorized or mandated by law. If the data is to be used for other purposes, then the public must be provided notice of those other uses.

These procedures do not in themselves create any legal rights, but are intended to

express the full and sincere commitment of the Air Force to protect individual privacy rights and which provide redress for violations of those rights.

#### *Data in the System*

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

#### *Access to the Data*

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

#### *Attributes of the Data*

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