more automated systems that may include DoD, another Federal agency, or a state or other local government. A system manager proposing a match that could result in an adverse action against a Federal employee must meet these requirements of the Privacy Act:

(1) Prepare a written agreement between participants;

(2) Secure approval of the Defense Data Integrity Board;

(3) Publish a matching notice in the FEDERAL REGISTER before matching begins;

(4) Ensure full investigation and due process; and

(5) Act on the information, as necessary.

(a) The Privacy Act applies to matching programs that use records from: Federal personnel or payroll systems and Federal benefit programs where matching:

(1) Determines Federal benefit eligibility;

(2) Checks on compliance with benefit program requirements;

(3) Recovers improper payments or delinquent debts from current or former beneficiaries.

(b) Matches used for statistics, pilot programs, law enforcement, tax administration, routine administration, background checks and foreign counterintelligence, and internal matching that won't cause any adverse action are exempt from Privacy Act matching requirements.

(c) Any activity that expects to participate in a matching program must contact Air Force Chief Information Officer/P immediately. System managers must prepare a notice for publication in the FEDERAL REGISTER with a Routine Use that allows disclosing the information for use in a matching program. Send the proposed system notice to Air Force Chief Information Officer/P. Allow 180 days for processing requests for a new matching program.

(d) Record subjects must receive prior notice of a match. The best way to do this is to include notice in the Privacy Act Statement on forms used in applying for benefits. Coordinate computer matching statements on forms with Air Force Chief Information Officer/P through the Major Command Privacy Act Officer.

§ 806b.51 Privacy and the Web.

Do not post personal information on publicly accessible DoD web sites unless clearly authorized by law and implementing regulation and policy. Additionally, do not post personal information on .mil private web sites unless authorized by the local commander, for official purposes, and an appropriate risk assessment is performed. *See* Air Force Instruction 33–129 *Transmission of Information Via the Internet.*[11]

(a) Ensure public Web sites comply with privacy policies regarding restrictions on persistent and third party cookies, and add appropriate privacy and security notices at major web site entry points and Privacy Act statements or Privacy Advisories when collecting personal information. Notices must clearly explain where the collection or sharing of certain information is voluntary, and notify users how to provide consent.

(b) Include a Privacy Act Statement on the web page if it collects information directly from an individual that we maintain and retrieve by his or her name or personal identifier (*i.e.,* Social Security Number). We may only maintain such information in approved Privacy Act systems of records that are published in the FEDERAL REGISTER. Inform the visitor when the information is maintained and retrieved by name or personal identifier in a system of records; that the Privacy Act gives them certain rights with respect to the government's maintenance and use of information collected about them, and provide a link to the Air Force Privacy Act policy and system notices at *http://www.foia.af.mil.*

(c) Anytime a web site solicits personally-identifying information, even when not maintained in a Privacy Act system of records, it requires a Privacy Advisory. The Privacy Advisory informs the individual why the information is solicited and how it will be used. Post the Privacy Advisory to the web page where the information is being solicited, or through a well-marked hyperlink ''Privacy Advisory—

[11] *http://www.e-publishing.af.mil/pubfiles/af/33/afi33-129/afi33-129.pdf.*

Please refer to the Privacy and Security Notice that describes why this information is collected and how it will be used.''

Subpart M—Training

§ 806b.52 Who needs training.

The Privacy Act requires training for all persons involved in the design, development, operation and maintenance of any system of records. More specialized training is needed for personnel who may be expected to deal with the news media or the public, personnel specialists, finance officers, information managers, supervisors, and individuals working with medical and security records. Commanders will ensure that above personnel are trained annually in the principles and requirements of the Privacy Act.

§ 806b.53 Training tools.

Helpful resources include:

(a) The Air Force Freedom of Information Act Web page which includes a Privacy Overview, Privacy Act training slides, the Air Force systems of records notices, and links to the Defense Privacy Board Advisory Opinions, the DoD and Department of Justice Privacy web pages. Go to *http://www.foia.af.mil*. Click on ''Resources.''

(b) ''The Privacy Act of 1974,'' a 32-minute film developed by the Defense Privacy Office. Contact the Joint Visual Information Activity at DSN 795–6543/7283 or commercial (717) 895–6543/7283, and ask for #504432 ''The Privacy Act of 1974.''

(c) A Manager's Overview, What You Need to Know About the Privacy Act. This overview gives you Privacy Act 101 and is available on-line at *http://www.foia.af.mil*.

(d) Training slides for use by the Major Command and base Privacy Act officers, available from the Freedom of Information Act web page at *http://www.foia.af.mil*, under ''Resources.''

NOTE: Formal school training groups that develop or modify blocks of instruction must send the material to Air Force Chief Information Officer/P for coordination.

§ 806b.54 Information collections, records, and forms or information management tools (IMT).

(a) Information Collections. No information collections are required by this publication.

(b) Records. Retain and dispose of Privacy Act records according to Air Force Manual 37–139, Records Disposition Schedule.[12]

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

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

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

APPENDIX A TO PART 806b—DEFINITIONS

Access: Allowing individuals to review or receive copies of their records.

Amendment: The process of adding, deleting, or changing information in a system of records to make the data accurate, relevant, timely, or complete.

Computer matching: A computerized comparison of two or more automated systems of records or a system of records with non-Federal records to establish or verify eligibility for payments under Federal benefit programs or to recover delinquent debts for these programs.

Confidential source: A person or organization giving information under an express or implied promise of confidentiality made before September 27, 1975.

Confidentiality: An expressed and recorded promise to withhold the identity of a source or the information provided by a source. The Air Force promises confidentiality only when the information goes into a system with an approved exemption for protecting the identity of confidential sources.

Cookie: Data created by a Web server that is stored on a user's computer either temporarily for that session only or permanently on the hard disk (persistent cookie). It provides a way for the Web site to identify users and keep track of their preferences. It is commonly used to ''maintain the state'' of the session. A third-party cookie either originates on or is sent to a Web site different from the one you are currently viewing.

[12] *http://www.e-publishing.af.mil/pubfiles/af/37/afman37-139/afman37-139.pdf*.