DEPARTMENTAL DIRECTIVE

Distribution:
All Department of Education Employees

Approved by: /s/ Scott Anderson for
Michell Clark
Assistant Secretary for Management

The Privacy Act of 1974
(The Collection, Use, and Protection of Personally Identifiable Information)

Table of Contents

For technical questions regarding this directive, please contact Lee Eiden via email or on 202-245-6454.

Supersedes ACS OCIO:1-101, **"**The Privacy Act of 1974 (The Collection, Use, and Protection of Personally Identifiable Information)," dated 1/10/2005.

I. Purpose

This directive establishes policy and procedures for protecting the privacy of individuals who are identified in the United States Department of Education (ED)'s Privacy Act Systems of Records and informs ED employees and officials of their rights and responsibilities under the Privacy Act of 1974, as amended (5 U.S.C. §552a) (Privacy Act). This directive supplements ED's regulations in Part 5b, Title 34, Code of Federal Regulations (C.F.R.).

II. Policy

ED will safeguard personal privacy in its collection, maintenance, use and dissemination of information about individuals and make such information available to the individual in accordance with the requirements of the Privacy Act.

III. Authorization

- The Privacy Act of 1974, 5 U.S.C. § 552a, as amended, available at http://www.usdoj.gov/foia/privstat.htm;
- ED's Privacy Act Regulations published at 34 C.F.R. Part 5b, available at http://www.gpoaccess.gov/C.F.R./index.html (search term=34CFR5b);
- Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch 36), available at http://www.whitehouse.gov/omb/egov/about_leg.htm#egov; high-level summary available at http://www.ed.gov/policy/gen/leg/egov.html.

IV. Applicability

This directive applies to all ED employees and all contractors who operate a Privacy Act System of Records for or on behalf of ED.

V. Definitions

A.	*Individual*	A living person who is a citizen of the United States or an alien lawfully admitted for permanent residence. A sole proprietorship, partnership, corporation or a business firm identified by the name of one or more persons is not an individual.
B.	*Information Technology (IT)*	As defined in the Clinger-Cohen Act, IT is any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

C.	*Maintain*	When used in connection with the term "record," maintain means to keep, collect, use, or disseminate. When used in connection with the term "System of Records," maintain means to have control over or responsibility for a System of Records.
D.	*Major information system*	An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.
E.	*Personal Identifier*	Name, Social Security Number, fingerprint, voice print, photograph, or any other coding device that correlates directly to an individual.
F.	*Personal Information*	Any information about an individual that bears the individual's name or other personal identifier, whether collected for a paper-based or computer-based information system.
G.	*Privacy Act Coordinators*	Individual(s) who are designated by a Principal Office (PO) to manage and coordinate the PO's responses to Privacy Act requests. Also see *System Manager*.
H.	*Privacy Act Issuances*	Compilations maintained by the Government Printing Office that describe Federal agency Systems of Records maintained on individuals. These issuances describe the system of records, including, but not limited to, the routine use disclosures that are permitted and the measures that are taken to safeguard the records. Updates to the most recent compilation are published by agencies in the *Federal Register*. The Issuances are available at http://www.access.gpo.gov/su_docs/aces/PrivacyAct.shtml and at http://www.ed.gov/policy/gen/leg/issuances03.doc. Also see *System Notice.*
I.	*Privacy Impact Assessment (PIA)*	An analysis of how information is handled: 1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, 2) to determine the risks and effects of collecting, maintaining and disseminating information in an identifiable form in an electronic information system, and 3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. Office of Management and Budget (OMB) guidance on PIA requirements is available at http://www.whitehouse.gov/omb/memoranda/m03-22.html.

		Current guidance that is specific to ED is available from the Office of Management (OM) Regulatory Information Management Services (RIMS) Privacy Officer or from the Computer Security Officer listed for each PO on ConnectED.
J.	*Record*	Any item, collection, or grouping of information pertaining to an individual and maintained by ED, including, but not limited to, the individual's education, financial transactions, medical history, and criminal or employment history, and containing a personal identifier.
K.	*Routine Use Disclosure*	The disclosure of a record without the consent of the subject individual, if such disclosure is described in and authorized by the System Notice and is compatible with the purpose for which the record was collected.
L.	*Significant Alteration of a System of Records*	A System of Records which has been changed in a way that is not minor, such as: 1) an increase in the number or a change in the types of individuals on whom records are maintained; 2) an expansion in the types or categories of information maintained; 3) a change that alters the purpose for which the information is used; 4) a change to equipment configuration (either hardware or software) that creates substantially greater access to the records in the system; 5) any addition or an exemption under section (j) or (k) of the Privacy Act; and/or 6) the addition of a routine use pursuant to 5 U.S.C. § 552a(b)(3). Significant alterations require a new System Notice and Report.
M.	*System Manager*	The ED official who is responsible for the management of a particular System of Records, and who is listed as such in the System Notice. A contractor cannot act as a System Manager.
N.	*System Notice*	A notice published in the *Federal Register* that describes the attributes of a System of Records.
O.	*System of Records*	Any group of records under ED's control from which information is retrieved by a personal identifier. Single records or groups of records that are not retrieved by a personal identifier are not part of a System of Records. Papers maintained by ED employees that are prepared, maintained, or discarded at the discretion of the employee and that are not subject to the Federal Records Act (44 U.S.C. § 2901), are not part of a System of Records—provided that such personal papers are not used by the employee or ED to determine any rights, benefits, or privileges of individuals.

P. *System Report* For a new System of Records or for a significant alteration of a System of Records, a system report is required to be submitted to the Office of Management and Budget (OMB), the Chair of the Senate Committee on Governmental Affairs, and the Chair of the House Committee on Government Reform.

VI. Responsibilities

A. Assistant Secretary for Management (ASM)

The Assistant Secretary for Management is ED's principal contact for privacy policies, and is responsible for coordinating implementation of OMB web and privacy policy and guidance. The ASM shall provide overall management and policy guidance to ED's Privacy Act Program. The ASM approves new and altered Privacy Act System of Records notices for submission to OMB and Congress and publication in the *Federal Register*. Finally, the ASM is ED's Privacy Appeals Officer and is responsible for deciding all written appeals of refusals to correct or amend records covered by the Privacy Act.

B. Regulatory Information Management Services (RIMS) Privacy Officer

The OM/RIMS Director is the Privacy Officer and is responsible for managing ED's Privacy Act Program. The Privacy Officer administers activities related to the establishment, alteration or termination of Systems of Records. In this capacity, the Privacy Officer or designee shall:

1. Review new and altered Privacy Act System Notices and System Reports for ASM approval, submission to OMB and Congress, and publication in the *Federal Register;*

2. Review all PIAs to ensure that they meet the requirements of Section 208 of the E-Government Act of 2002, approve the PIA documentation, and make it publicly available, either in the *Federal Register* notice or on ED's Web site (www.ed.gov);

3. Review and approve regulations and directives regarding Privacy Act administration;

4. Establish a program to periodically review record-keeping policies and practices within ED, in compliance with the Privacy Act;

5. Consult with the Office of General Counsel (OGC) on all legal matters related to implementation of the Privacy Act within ED;

6. Develop procedures and documents required to implement the Privacy Act, including reporting formats, directives, reports, and handbooks, in compliance with the Privacy Act, ED regulations, and OMB Guidelines;

7. Provide technical assistance to system and program managers, as needed, in the development of the documentation required for System Notices, System Reports, Privacy Act statements, and PIAs;

8. Ensure that the rules governing employee conduct, training and implementation of the Privacy Act requirements are current and sufficient;

9. Coordinate the preparation of an annual report to OMB on Section 208 of the E-Government Act of 2002 (Public Law 107-347 44, U.S.C. Ch. 36); and

10. Prior to consideration of all computer-matching agreements by ED's Data Integrity Board, review all the agreements for computer matching programs under 5 U.S.C. § 552a(o) to ensure compliance with ED policy, OMB Guidelines, and the Computer Matching and Privacy Protection Act of 1988.

C. Principal Officers

Principal Officers shall:

1. Implement the Privacy Act and the requirements specified in this directive within their respective areas. They are responsible for designating an appropriate ED employee to serve as System Manager for an existing or proposed System of Records;

2. Designate a PO Privacy Act Coordinator to ensure compliance with the Privacy Act;

3. Ensure that all requests from subject individuals for notification, access and amendment are processed promptly;

4. Coordinate activities necessary to assist OM RIMS in making reports under the Privacy Act; and

5. Ensure that all employees and contractors who design, develop, or maintain a Privacy Act System of Records to accomplish an ED function are aware of their responsibility for protecting information on individuals that is in identifiable form.

D. Privacy Act Coordinators

Privacy Act Coordinators shall:

1. Send the requestor a written acknowledgement of receipt of a Privacy Act written request within ten business days of receipt (a request is not officially received for purposes of response deadlines until proof of identification has been received);

2. Assign each Privacy Act request to the appropriate System Manager and coordinate the response to the requester; and

3. Ensure that the individual requesting copies of his or her records provides proper identification in accordance with 34 C.F.R. §5b.5(b) prior to release of personally identifiable information. (RIMS will perform such identification for ED Management and Staff Offices.)

E. System Managers

System Managers shall:

1. Establish information collection parameters to ensure that only such information necessary to carry out the function of the system is collected (See Section VII.B. of this document); consult the ACS directive on "Information Collection Activities and Burden Control" for guidance about advance clearance of information collection activities; review information collection instruments to ensure compliance, and consult with the RIMS Privacy Officer regarding the need for a Privacy Act System Notice, System Report, Privacy Act statement, and PIA.

2. Familiarize themselves with ED/OCIO Information Assurance handbooks, IT Investment Management guidance, and PO Computer System Officer guidance. Additional information that is relevant to carrying out the provisions of the Privacy Act, especially as it relates to PIAs, may be found in these documents.

3. Prepare a PIA when initiating, consistent with the Paperwork Reduction Act, a new electronic information collection of information on 10 or more persons (excluding employees of the federal government), or when developing or procuring a new information technology system or project where information about members of the public will be collected, maintained, or disseminated in an identifiable form. When undertaking a new electronic information collection, the PIA may be conducted and submitted to OMB, and made publicly available, as part of the OMB 83-I Supporting Statement (the request to OMB to approve a new agency information collection);

4. Ensure administrative, technical, and physical controls to safeguard the storing and transmitting of records;

5. Provide subject individuals with the opportunity to correct inaccuracies in their record when they request the opportunity to do so, unless a system has been legally exempted from this requirement. If the request for amendment is denied, inform the subject individual of the denial and the reasons for the denial, and of his or her rights to appeal the denial;

6. Maintain an accounting of all disclosures made from the System of Records, except disclosures required by the Freedom of Information Act (FOIA) or to those officers and employees in ED who have a need for the record in the performance of their duties, unless a system has been legally exempted from this requirement.

7. Determine duplication fees to be charged in accordance with 34 C.F.R. Part 5b (See VII.I., Fees Under the Privacy Act); and

8. Ensure that applicable Web-based systems comply with Section 208 of the E-Government Act of 2002 to include machine-readable notices for P3P (Platform for Privacy Preferences).

F. General Counsel

The General Counsel is responsible for interpreting the Privacy Act and reviewing Privacy Act notices, regulations, policy statements and related documents for legal form and substance.

G. Inspector General

The Inspector General has the authority to make written requests to another agency or to any instrumentality of the U.S. Government for records related to a legally authorized Office of Inspector General civil or criminal law enforcement activity, pursuant to subsection (b)(7) of 5 U.S.C. § 552a.

The Inspector General has the authority to request information covered by the Privacy Act, for the purpose of carrying out the duties of the office, from any Principal Office, and the Principal Office may disclose the requested information to the Inspector General.

H. Contractors

Contractors and their employees who design, develop, or maintain a system of records on behalf of ED to accomplish an ED function are subject to the Privacy Act, including its criminal provisions, as well as the ED employee standards of conduct contained at 34 C.F.R. Part 5b. All ED contracts that provide for the

design, development, or operation of a system of records on behalf of ED to accomplish an ED function must contain provisions from the Federal Acquisition Regulations that apply the requirements of the Privacy Act of 1974 and OMB Circular No. A-130 to Government contracts. These provisions from the Federal Acquisition Regulations are contained at 48 C.F.R. Subpart 24.1 and 48 C.F.R. Sections 52.224-1 and 52.224-2. When a Government contract provides for the operation of a system of records to accomplish an agency function, the contractor and any employee of the contractor is considered to be an employee of the agency.

VII. Procedures and Requirements

A. Basic Requirements of the Privacy Act

1. At least 40 days prior to creation of a new System of Records or significant alteration to an existing system, ED must submit documentation to OMB and the Congress, and publish a notice of the system in the *Federal Register*. Enough time must be allotted for preparing the document for publication.

2. Each time ED asks individuals to supply information to be used in a System of Records, the System Manager must provide the individual with a written "Privacy Act statement" that can be retained by the individual. This Privacy Act statement must inform the individual of the legal authority for collecting the information; whether disclosure of such information by the individual is mandatory or voluntary; the principal purpose(s) for which the information is being collected and the routine uses which may be made of the information; and the effect on the individual if the individual does not provide the information. If ED requests that individuals provide their Social Security Numbers, ED shall inform the individuals whether the disclosure is mandatory or voluntary, by what authority it is solicited, and what uses will be made of it.

3. Unless a System of Records has been exempted from this requirement, to the greatest extent practicable, information about an individual must be collected directly from the individual if the information may be used to make decisions with respect to the individual's rights, benefits, and privileges under Federal programs.

4. Unless a System of Records has been exempted from this requirement, the information ED collects and maintains about individuals must be both relevant and necessary to accomplish ED's purpose, as required by statute or Executive Order.

5. Unless a System of Records has been exempted from this requirement, the information that is maintained in a System of Records must be kept as

accurate, relevant, current, and complete as possible to assure fairness to the individual.

6. Unless a System of Records has been exempted from this requirement, an individual generally has a right to see records about himself or herself that are contained in a System of Records.

7. Unless a System of Records has been exempted from this requirement, if an individual believes records about himself or herself are inaccurate, irrelevant, untimely, incomplete or unnecessary to ensure fairness, the individual may ask the System Manager to amend the records. (See VII., G. and H.)

8. ED cannot disclose a record in a System of Records without the individual's prior written consent unless the disclosure is:

   a. To an ED employee who has a "need-to-know" in the performance of an official duty.

   b. Required under the FOIA. (See ACS Directive OCIO:1-102.)

   c. Authorized under a "routine use" of the System of Records.

   d. Permitted under other conditions of disclosure of the Privacy Act, such as an emergency affecting the health or safety of the individual (See Appendix F and 5 U.S.C. § 552a(b)(4)-(12)).

9. ED must keep an accounting of every disclosure it makes (except for disclosures to officers or employees who have a need-to-know or under FOIA) and, with limited exceptions, provide the accounting to an individual upon request.

10. As indicated, requirements 3-7 and 9 above do not apply if a system has been legally exempted from this requirement. ED has exempted certain systems of records maintained by the Office for Civil Rights, Office of Inspector General and the Office of Management.

B. New System of Records

A new System of Records is one for which no public notice previously has been published in the *Federal Register*. A new System of Records is created whenever:

1. A program, authorized by either a new or existing statute or Executive Order, requires for its successful accomplishment the creation and retrieval of personally identifiable records;

2. There is a proposed new use of existing records that is incompatible with the purposes for which the records were originally collected. In this case, all individuals covered by the existing System of Records must be notified through a notice in the *Federal Register* of the new purpose and routine uses for the records in the system and must be provided with a new Privacy Act statement; and/or

3. There is a new organization of records, resulting in the consolidation of two or more existing systems into one new ("umbrella") system, whenever the consolidation cannot be classified under a current System Notice.

C. Significant Alteration of a System of Records

The significant alteration of an existing System of Records requires an altered System Notice and a System Report. A System of Records is considered to be significantly altered when a change to the System of Records will:

1. Increase or change the number or types of individuals on whom records are maintained. An increase attributable to normal growth need not be reported;

2. Expand the types or categories of information maintained;

3. Alter the purpose for which the information is used;

4. Change the equipment (either hardware or software) that creates substantially greater access to personally identifiable information in the System of Records;

5. Add an exemption under Section (J) or (K) of the Privacy Act; and/or

6. Add a routine use under 5 U.S.C. § 552a(b)(3).

Minor changes that alter the System of Records may require an altered System Notice but do not require a System Report. Examples of minor changes are:

1. A change in the designation of the System Manager due to a reorganization, as long as an individual's ability to gain access to his or her records is not affected;

2. Changing applicable safeguards as a result of a risk analysis or review of security; or

3. Discontinuing a routine use when there is no longer a need for the authorized disclosure.

D. Procedures for Processing a New or Altered System of Records Notice

1. The System Manager planning to create or alter a System of Records should consult the OM RIMS Privacy Officer as well as the Information Collection Activity staff (See ACS directive "Information Collection Activities and Burden Control" and "A Guide to the Information Collection Clearance Process"). In addition, current guidance from ED's Information Assurance team, IT Investment Management team, and the PO Computer Security Officer must be consulted.

2. The System Manager prepares the following documentation and transmits an electronic copy of the documentation to the OM RIMS Privacy Officer:

   a. *Federal Register* Notice (See Appendix A for instructions);

   b. System Report (See Appendix B for instructions);

   c. Transmittal Letter (See Appendix C for instructions);

   d. The Privacy Act Statement that is made publicly available to individuals, if needed (See Appendix D for instructions); and

   e. A PIA document, if needed (See Appendix E for instructions).

3. The OM RIMS Privacy Officer reviews the documentation and transmits it to OGC for appropriate concurrence and ED's clearance, and communicates the outcome to the System Manager. Note: Currently, only items a, b, and c are sent to OGC/Division of Regulatory Services to circulate for ED clearance.

4. The System Manager submits the final package to the RIMS Privacy Officer.

5. The RIMS Privacy Officer obtains the ASM's signature where needed and submits the signed package to OGC for transmittal to the *Federal Register* for publication, OMB, and Congress.

E. Timing and Distribution of New and Altered System Reports

1. Timing of the report submission involves two stages: (1) ED clearance, and (2) submission to Congress and OMB. The latter may be done on the same day as the System Notice is submitted to the *Federal Register* for publication.

2. ED clearance requires that the report and PIA be submitted to the OM RIMS Privacy Officer no less than 120 calendar days prior to planned implementation, in order to allow for administrative and legal review in preparation for the approval of the ASM.

3. OMB policy and the Privacy Act require that the system report be forwarded to Congress and OMB 40 days prior to implementation, unless compelling circumstances justify a waiver from OMB of 10 days of the 40-day period.

4. Review by the public requires that the new or altered System Notice be published in the *Federal Register* no less than 30 calendar days before any routine use disclosures are made pursuant to 5 U.S.C. §552a(b)(3).

5. If OMB does not act on the report within 40 days from the transmittal date, ED may implement the System of Records. If OMB takes action within the 40-day time period to prevent implementation of the notice, ED shall not use the System of Records until all issues with OMB have been resolved.

6. The System Notice must be submitted for publication in the *Federal Register* at the same time or before the new or altered system report is sent to OMB and the Congress.

7. If ED plans to exempt the System of Records from certain provisions of the Privacy Act under 5 U.S.C. §552a(j) or (k), ED must publish in the *Federal Register* an amendment to its Privacy Act Regulations at 34 C.F.R. Part 5b and OMB must approve the amendments. After the regulations are effective, the Principal Office must develop a System of Records notice that will include a list of the provisions from which the system is exempted.

8. The 40-day review and comment period for OMB and Congress, and the 30-day public comment period for routine uses may run concurrently.

F. Privacy Impact Assessment

1. The E-Government Act of 2002 implemented the PIA as a requirement. The purpose of Section 208 of the E-Government Act is to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic government. The PIA process requires ED to review how information about individuals is handled when ED uses information technology to collect new information or when ED

develops or buys new IT systems to handle collections of personally identifiable information.

2. The Privacy Impact Assessment can be submitted with a related Information Collection Request (ICR) to OMB for approval. Once the RIMS Privacy Officer has approved the PIA, it can be published in the *Federal Register* at the same time the System of Records notice is published in the *Federal Register*, or it can be posted to the system's web site with the web site privacy policy.

3. The goals of the PIA include:

   a. Providing ED senior management with the tools to make informed policy and system design or procurement decisions based on an understanding of privacy risk and of options available for mitigating that risk;

   b. Ensuring that system and program managers are accountable for the proper handling of privacy issues;

   c. Establishing a consistent format and structured process for analyzing both technical and legal compliance with applicable privacy laws and regulations, as well as accepted privacy policy;

   d. Providing basic documentation on the flow of personal information within ED systems for use and review by policy and program staff, management staff, systems analysts, and security specialists; and

   e. Providing the American public with assurances that their personal information is protected by ED.

G. Processing Privacy Act Requests for Access

1. An individual may ask ED if it maintains a record about the individual and, at the same time, ask for access to that record. The procedures for these types of requests are contained in 34 C.F.R. Part 5b.5. These requests may be made in person by the individual or in writing. If the request is made in person, the individual may have another individual accompany him or her.

2. An individual's request for access to his or her own records under the Privacy Act also must be handled as a request under the FOIA, 5 U.S.C. §552.

3. A Privacy Act Coordinator or a System Manager shall require an individual requesting access to his or her records to provide verification of identity as required in 34 C.F.R. §5b.5(b). (RIMS will perform such identification for ED Management and Staff Offices.)

4. A parent or legal guardian is authorized to act on behalf of any minor child or on behalf of any individual who has been declared by a court of competent jurisdiction to be incompetent due to mental or physical incapacity or age. A parent or legal guardian who acts on behalf of an incompetent shall verify his or her identity as required by 34 C.F.R. §5b.5(b)(2)(iii).

5. An individual may appeal an initial denial for access to his or her records, in accordance with 34 C.F.R. §5b.8. The appeal should be forwarded to the RIMS Privacy Act Officer(s).

6. If an individual prevails on an administrative appeal, he or she will be informed by RIMS in writing that the requested records will be forthcoming.

7. If the initial denial is supported in whole or part on an administrative appeal, the individual will be notified in writing of (a) the decision to uphold the initial denial; and (b) the provision for judicial review under section 552a(g)(1) of the Privacy Act.

H. Processing Privacy Act Requests for Correction or Amendment

1. An individual may request correction or amendment of any record pertaining to himself or herself if the record is in a System of Records maintained by ED. The individual may make a request by submitting the following information in writing:

    a. The name of the individual making the request;

    b. The name of the system, as described in the *Federal Register*, if known;

    c. The particular record which the individual is seeking to correct or amend;

    d. A description of the correction or amendment requested and the reason for the request; and

    e. Verification of identity (e.g., driver's license, voter registration card) in accordance with 34 C.F.R. §5b.5(b).

2. Within 10 business days of receipt of the request, the System Manager will acknowledge receipt of the request. Within 30 business days, the System Manager should:

   a. Make the correction, deletion, or addition; advise the individual of the determination to do so; notify prior recipients of the record outside ED of the amendment in accordance with the accounting procedures of the Privacy Act and make annotation of the occurrence and substance of the correction/amendment in the accounting; or

   b. Inform the individual that the request is denied, the reason for denial, and that the individual can appeal in writing.

   c. If the initial denial is reversed on administrative appeal, the individual and the System Manager will be informed in writing that the record or a portion of the record will be amended. The System Manager shall make such amendment; notify prior recipients of the record outside ED of the amendment, in accordance with the accounting requirements of the Privacy Act; and make notation of the occurrence and substance of the amendment.

   d. If the denial is upheld in whole or in part, the individual will be informed: (a) of the determination and its basis; and (b) of the individual's right to file a concise statement of reasons for disagreeing with ED's position and the procedure for doing so.

   e. Final determination on appeals for correction or amendment will be made not later than 30 business days from the date on which the individual requests the review unless, for good cause, the appeal authority extends the period and notifies the individual.

I. Fees Under the Privacy Act

1. No fees will be charged for search and review time.

2. Fees will be charged for additional copies made according to the fee schedule contained in 34 C.F.R. Part 5b.13(b) such as:

   a. Copying records capable of being photocopied; or

   b. Copying records not capable of being photocopied (e.g., diskettes, CDs or magnetic tapes) at actual cost to be determined on a case-by-case basis. If fees total more than $25, the requestor will be

notified and may be required to pay the fees before the records are provided.

c. Fees (checks, bank drafts, or money orders) should be made payable to the U.S. Department of Education. Each such receipt must be annotated "Privacy Act Request." The applicable system manager's name/office should be included on the reference/note line.

d. Privacy Act requestors must submit fees (checks, bank drafts, or money orders) directly to:

U.S. Department of Education
Office of the Chief Financial Officer
Financial Management Operations
400 Maryland Avenue S.W.
Washington, DC 20202

e. The Office of the Chief Financial Officer will notify RIMS of payments received.

VIII. Civil Actions and Criminal Penalties

All ED employees and contractors have responsibilities to prevent the improper disclosure of records that are subject to the Privacy Act. Willful violation of the Privacy Act can result in criminal sanctions against an employee or contractor and civil liability for ED and its contractors.

A. Civil Actions

Any individual may sue ED if there has been improper use of records or failure to comply with the Privacy Act. Any of the following actions by ED employees or contractors may subject ED to a civil action:

1. Failure to Amend

If the appeal authority refuses an appeal to amend or correct an individual's record in accordance with his or her request, ED may be subject to a civil action.

2. Failure to Provide Access

If a System Manager refuses to comply with an individual's request for notification of, or access to, a record pertaining to him or her, ED is subject to civil liability.

3. Failure to Maintain Accuracy

If a System Manager fails to maintain records on an individual that are accurate, timely, relevant, and complete, resulting in an adverse determination with respect to that individual's qualifications, character, rights, opportunities or benefits, ED may be subject to a civil action.

4. Failure to Comply with Any Other Provision of the Privacy Act

If an ED employee fails to comply with any other provision of the Privacy Act or its regulations, resulting in an adverse effect on an individual, ED may be subject to a civil action.

B. Criminal Penalties

An ED or contractor employee may be personally subject to criminal penalties as set forth below and in 5 U.S.C. § 552a(i):

1. Improper Disclosure of Records

Any officer or employee who, by virtue of his or her employment or in his or her official position, has possession of, or access to, agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or 34 C.F.R. Part 5b and who, knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

2. Failure to Publish a System of Records Notice

Any officer or employee who willfully maintains a System of Records without meeting the notice requirements of the Privacy Act shall be guilty of a misdemeanor and fined not more than $5,000.

3. Obtaining a Record Under False Pretenses

Any person, whether or not an ED employee, who knowingly and willfully requests or obtains any record concerning an individual from ED under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

C. Disciplinary Sanctions Against ED Employees

Any ED employee who fails to comply with the employee standards of conduct in Appendix A to 34 C.F.R. Part 5b is subject to disciplinary action for that failure.

Appendix A: The *Federal Register* Notice for a New or Altered System of Records

The Office of the Federal Register has established items of information that must appear in a *Federal Register* notice for a new or altered System of Records. These items are listed below in the order that they must appear in the System Notice (See attached pages)

1. **System Number** (assigned by the OM RIMS Privacy Officer).

2. **System Name**: Provide the official name of the System of Records.

3. **Security Classification**: None in ED.

4. **System Location**: Specify each address at which the System is maintained. Include Headquarters and Regional locations and the addresses of contractors, if any, who may maintain the System for ED.

5. **Categories of Individuals Covered by the System**: Describe the categories of individuals on whom records are maintained in sufficient detail so as to enable individuals to determine if there is information on them in the System.

6. **Categories of Records in the System**: Give a brief description of all of the types of information in the System.

7. **Authority for Maintenance of the System**: Cite the specific statute(s) and/or Executive order(s) that authorizes ED to maintain the System.

8. **Purpose(s):** State the reason(s) for creating the System and what the System is designed to accomplish.

9. **Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses**: Describe each routine use that will be made of the records, including the categories of users and the purpose of each use.

10. **Disclosure to Consumer Reporting Agencies:** State whether such disclosure, regarding a claim by the Department which is determined to be valid and overdue (as specified in U.S.C. §552a(b)(12) and 31 U.S.C. §3711(e)), will be made.

11. **Policies And Practices For Storing, Retrieving, Accessing, Retaining, And Disposing Of Records In The System:** Describe same.

12. **Storage**: List all media in which records in the System are maintained (e.g., file folders, magnetic tape, microform, etc.). Briefly describe how each medium is stored.

13. **Retrievability**: Describe how the records are indexed and retrieved.

14. **Safeguards**: Describe your security policies and the procedures in place to prevent unauthorized disclosure of the records. Include the categories of ED employees to whom access will be limited.

15. **Retention and Disposal**: Indicate how long ED retains the records in identifiable form and how ED will dispose of the records. Ensure that an approved Records Control Schedule covers the records.

16. **System Manager(s) and Address**: Provide the title and complete business address of the person responsible for the records. A contractor, consultant, or anyone other than an ED employee may not be designated as a System Manager.

17. **Notification Procedure**: Provide the procedural information necessary for an individual to find out whether or not there are records about him/her in the System. Provide the complete address of the System Manager to which requests for notification may be presented. Do not include telephone numbers.

18. **Record Access Procedures**: Provide the procedural information necessary for an individual to gain access to records about him/herself. Give name and address of the System Manager whom the individual should contact if he or she wants to gain access to any record about him- or herself in the System.

19. **Contesting Record Procedures**: Provide procedures for an individual to contest the accuracy, relevancy, completeness and timeliness of records about him/herself. Give name and address of the System Manager to be contacted.

20. **Record Source Categories**: Describe the sources from which the information in the System is obtained. Sources include, but are not limited to, the individual on whom the records are maintained, previous and current employers, educational institutions, local governments, and other agencies.

21. **Exemptions Claimed for the System**: Under limited circumstances, the Privacy Act permits agencies to exempt a System of Records from compliance with certain provisions of the Privacy Act. Identify the Privacy Act exemptions(s), by subsection of the Privacy Act, that are applicable to the System; provisions of the Privacy Act being exempted; and a brief statement of the reason for invoking the exemption. Cite the *Federal Register* issue and page number where the proposed rule creating the exemption was published. If no exemptions are applicable, enter “none.”

Appendix B: System Report (Report to OMB and Congress)

The narrative statement should be brief. The statement should:

1. Describe the purpose for which ED is establishing the System of Records.

2. Identify the legislative and/or regulatory authority under which the System of Records is maintained.

3. Provide ED's evaluation of the probable or potential effects of the system implementation on the privacy of individuals.

4. Provide a brief description of the steps taken by ED to minimize the risk of unauthorized access to the System of Records.

5. Explain how each proposed routine use satisfies the compatibility requirement of subsection (a)(7) of the Privacy Act. For altered systems, this requirement pertains only to any newly proposed routine use.

6. Provide OMB Control Numbers, expiration dates, and titles of any OMB-approved ICRs (e.g. forms, surveys) contained in the System of Records. If the request for OMB clearance of the information collection is pending, give the title of the collection and the date it was submitted for clearance.

Appendix C: Transmittal Letters

1. The letter must be addressed to the Director, Office of Information and Regulatory Affairs at OMB and prepared for the signature of the Assistant Secretary for Management.

2. The letter must contain assurance that the proposed system does not duplicate any existing agency or government-wide System of Records.

3. The letter must state that duplicate copies of the documentation have been distributed to the Chairman of the Committee on Government Reform of the U.S. House of Representatives and the Chairman of the Committee on Governmental Affairs of the U.S. Senate.

4. If the System Manager believes a request to waive 10 days of the OMB review period is appropriate or if a program is mandated to meet a specified deadline date, the letter to OMB must include a request for a waiver of 10 of the 40-day review period and demonstrate compelling reasons for the waiver request.

Appendix D: Privacy Act Statement

This statement must be in writing and must inform the individual of the authority for collecting the information, the purpose for which the information is being collected on him/her and the routine uses that will be made of the information. The statement must also state whether furnishing information is voluntary or mandatory and explain what the consequences will be if an individual does not agree to furnish the information.

Appendix E: Privacy Impact Assessment (PIA)

As described in OMB implementation guidance on the E-Government Act, Section 208, Attachment A, agencies are required to conduct privacy impact assessments for electronic information systems and collections and, in general, make them publicly available.

The PIA must address:

1. What information is to be collected;

2. Why the information is being collected;

3. The intended use of the information by ED;

4. With whom the information will be shared;

5. What notice or opportunities for consent will be provided to individuals regarding what information is collected and how that information is shared;

6. How the information will be secured; and

7. Whether a System of Records is being created under the Privacy Act.

Reporting Requirements to OMB:

Each year, at the call of OMB, the OM RIMS Privacy Officer must prepare and submit a report of ED activities under the Privacy Act.

This report must address the following four elements:

1. *IT systems or information collections for which PIAs were conducted*. Include the mechanism by which the PIA was made publicly available (if made available in summary form or not at all, explain). If made available in conjunction with an ICR or System of Records notice, include the publication date of the PIA.

2. *Persistent tracking technology uses*. If the use of persistent tracking technology (e.g., "persistent cookies") is authorized, include the need that compels use of the technology, the safeguards instituted to protect the information collected, the agency official approving use of the tracking technology, and the text of the privacy policy notification of such use.

3. *Agency achievement of goals for machine readability*. Include goals for and progress toward achieving compatibility of privacy policies with machine-readable privacy protection technology.

4. *Contact information.* Include the individual(s) (name and title) appointed by the head of the Executive Department or agency to serve as the agency's principal contact(s) for IT/Web matters and the individual (name and title) primarily responsible for privacy policies.

Appendix F: Exceptions to the Privacy Act Prohibition Against Disclosure Without Prior Written Consent

1. **Internal Disclosures.** The System Manager may make disclosures to officers and employees of the Agency who have a need for the record in the performance of their duties as determined by the System Manager.

2. **Disclosures Required Under the Freedom of Information Act (FOIA).** Disclosures may be made under the Privacy Act when required by the FOIA if there is a written FOIA request. However, when a FOIA exemption – typically Exemption 6 or Exemption 7(C) – applies to a Privacy Act-protected record, the Privacy Act prohibits ED from making a "discretionary" FOIA release because the disclosure would not be "required" by the FOIA.

3. **Routine Use.** Disclosures may be made for a routine use as described and published in the *Federal Register* notice describing the System or Records so long as the routine use is compatible with the purpose for which the record was collected.

4. **Bureau of the Census.** Disclosures may be made to the Bureau of the Census for the purpose of planning or carrying out a census or survey or related activity.

5. **Statistical Research/Reporting.** Disclosures may be made to a recipient who has provided ED with advanced adequate written assurance that the record will be used solely for statistical research or as a reporting record, and that the record is to be transferred in a form that is not individually identifiable.

6. **Preservation of Records.** Disclosures may be made to the National Archives and Records Administration (NARA) of the United States of a record that has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by NARA to determine whether the record has such value.

7. **Civil or Criminal Law Enforcement.** Disclosures may be made to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the Agency specifying the particular portion of a record desired and the law enforcement activity for which the record is sought.

8. **Health or Safety.** Disclosures may be pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual.

9. **Congressional Disclosures.** Disclosures may be made to either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee or any such joint committee. This

exception does not apply to disclosures to individual members of Congress acting on his or her own behalf or on behalf of a constituent.

10. **Government Accountability Office (GAO).** Disclosures may be made to the Government Accountability Office for the purpose of carrying out the duties of that office.

11. **Court Order.** Disclosures may be made pursuant to the order of a court of competent jurisdiction.

12. **Debt Collection.** Disclosure may be made to a consumer reporting agency in accordance with Section 3(d) of the Federal Claims Collection Act of 1966 (31 U.S.C. §3701(a)(3)).