Maryland Avenue, SW., room 6E227, Washington, DC 20202–6110.

**NOTIFICATION PROCEDURE:**

If you wish to determine whether a record exists regarding you in the system of records, contact the system manager. Your request must meet the requirements of regulations in 34 CFR 5b.5, including proof of identity.

**RECORD ACCESS PROCEDURES:**

If you wish to gain access to your record in the system of records, contact the system manager at the address listed under **SYSTEM MANAGER AND ADDRESS**. Requests should contain your full name, address, and telephone number. Your request must meet the requirements of regulations in 34 CFR 5b.5, including proof of identity.

**CONTESTING RECORD PROCEDURES:**

If you wish to contest the content of a record regarding you in the system of records, contact the system manager. Your request must meet the requirements of the regulations in 34 CFR 5b.7, including proof of identity.

**RECORD SOURCE CATEGORIES:**

Information maintained in this system of records is obtained from anyone who chooses to voluntarily submit a public comment or supporting materials in response to a Department rulemaking document or notice, including individuals and representatives of Federal, State or local governments, businesses, and other organizations.

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**

None.

[FR Doc. E7–23058 Filed 11–26–07; 8:45 am]

**BILLING CODE 4000–01–P**

## DEPARTMENT OF EDUCATION

### Privacy Act of 1974; System of Records—Investigatory Material Compiled for Personnel Security, Suitability, Positive Identification Verification and Access Control for the Department of Education Security Tracking and Reporting System (EDSTAR)

**AGENCY:** Office of Management, Department of Education.

**ACTION:** Notice of altered and deleted systems of records.

**SUMMARY:** In accordance with the Privacy Act of 1974, as amended (Privacy Act), the Department of Education (Department), publishes this notice to amend and rename the system of records entitled ''Investigatory Material Compiled for Personnel Security and Suitability Purposes'' (18–05–17) as ''Investigatory Material Compiled for Personnel Security, Suitability, Positive Identification Verification and Access Control for the Department of Education Security Tracking and Reporting System (EDSTAR)'' (18–05–17) and to delete the system of records entitled ''Identification Media Records'' (18–05–16). The Department is taking these actions because these systems of records have been merged into and consolidated with the EDSTAR system of records.

EDSTAR is designed to implement the requirements of Homeland Security Presidential Directive (HSPD)–12. HSPD–12 is a Presidential directive that requires the promulgation of a Federal standard to ensure a common, governmentwide standard for secure and reliable forms of Personal Identity Verification (PIV). On February 25, 2005, the National Institute of Standards and Technology's (NIST's) Computer Security Division issued Federal Information Processing Standard (FIPS) 201, entitled ''Personal Identity Verification of Federal Employees and Contractors'', in order to satisfy the requirements of HSPD–12 to improve the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems.

The Department maintains records in EDSTAR for the purpose of making individual positive identification verification, adjudication determinations concerning suitability for Federal employment and contract positions, decisions concerning access to the Department's facilities and information systems, and information related to the issuance of PIV and FIPS compliant identification media and access to restricted areas. Because many of these records are currently covered by the systems of records entitled ''Identification Media Records'' (18–05–16) and ''Investigatory Material Compiled for Personnel Security and Suitability Purposes'' (18–05–17), the Department is merging and consolidating these systems of records by amending and renaming the ''Investigatory Material Compiled for Personnel Security and Suitability Purposes'' (18–05–17) system as EDSTAR and deleting the system of records for ''Identification Media Records'' (18–05–16).

**DATES:** We must receive your comments about the altered and deleted systems of records notice on or before December 27, 2007.

The Department filed a report describing the altered system of records covered by this notice with the Chair of the Senate Committee on Homeland Security and Governmental Affairs, the Chair of the House Committee on Oversight and Government Reform, and the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget (OMB) on November 21, 2007. The altered system of records will become effective at the later date of—(1) The expiration of the 40-day period for OMB review on December 31, 2007 or (2) December 27, 2007, unless the system of records needs to be changed as a result of public comment or OMB review.

**ADDRESSES:** Address all comments about the altered and deleted systems of records to Cecelia E. Briscoe, Senior Program Analyst, Security Services, Office of Management, Room 2W312, U.S. Department of Education, 400 Maryland Avenue, SW., Washington, DC 20202–5345. If you prefer to send comments through the Internet, use the following address: *Security.Services@Ed.gov.*

You must include the term ''EDSTAR Comments'' in the subject line of your electronic message.

During and after the comment period, you may inspect all public comments about this notice at the U.S. Department of Education in room 2W330, 400 Maryland Avenue, SW., Washington, DC, between the hours of 8 a.m. and 4:30 p.m., Eastern time, Monday through Friday of each week except Federal holidays.

**Assistance to Individuals With Disabilities in Reviewing the Rulemaking Record**

On request, we will supply an appropriate aid, such as a reader or print magnifier, to an individual with a disability who needs assistance to review the comments or other documents in the public rulemaking record for this notice. If you want to schedule an appointment for this type of aid, please contact the person listed under **FOR FURTHER INFORMATION CONTACT**.

**FOR FURTHER INFORMATION CONTACT:** Colette Hawley, Security Services, Office of Management, room 2W312, U.S. Department of Education, 400 Maryland Avenue, SW., Washington, DC 20202–5345. Telephone number: (202) 401–2993. If you use a telecommunications device for the deaf (TDD), you may call the Federal Relay Service (FRS) at 1–800–877–8339.

Individuals with disabilities may obtain this document in an alternative format (e.g., Braille, large print, audiotape, or computer diskette) on

request to the contact person listed in the preceding paragraph.

**SUPPLEMENTARY INFORMATION:**

**Introduction**

The Privacy Act (5 U.S.C. 552a(e)(4)) requires the Department to publish in the **Federal Register** this notice of an altered system of records maintained by the Department. The Department's regulations implementing the Privacy Act are contained in part 5b of title 34 of the Code of Federal Regulations (CFR).

The Privacy Act applies to information about individuals that is maintained in a system of records from which individually identifying information is retrieved by a unique identifier associated with each individual, such as a name or social security number. The information about each individual is called a ''record,'' and the system, whether manual or computer-based, is called a ''system of records.'' The Privacy Act requires each agency to publish notices of new or altered systems of records in the **Federal Register** and to submit reports to the Administrator of the Office of Information and Regulatory Affairs, OMB, the Chair of the House Committee on Oversight and Government Reform, and the Chair of the Senate Committee on Homeland Security and Governmental Affairs, whenever the agency publishes a new or altered system of records.

**Electronic Access to This Document**

You can view this document, as well as all other documents of this Department published in the **Federal Register**, in text or Adobe Portable Document Format (PDF) on the Internet at the following site: *www.ed.gov/news/fedregister.*

To use PDF you must have Adobe Acrobat Reader, which is available free at this site. If you have questions about using PDF, call the U.S. Government Printing Office (GPO), toll free, at 1–888–293–6498; or in the Washington, DC, area at (202) 512–1530.

**Note:** The official version of this document is the document published in the **Federal Register**. Free Internet access to the official edition of the **Federal Register** and the Code of Federal Regulations is available on GPO Access at: *www.gpoaccess.gov/nara/index.html.*

Dated: November 21, 2007.

**Michell C. Clark,**

*Assistant Secretary for Management.*

For the reasons discussed in the preamble, the Assistant Secretary for Management of the Department publishes a notice of altered and deleted systems of records to read as follows:

**DELETED SYSTEM OF RECORDS**

The Department identifies the system of records entitled Identification Media Records (18–05–16), as published in the **Federal Register** on December 26, 2002 (67 FR 78794–96), to be deleted because it has been merged into and consolidated with the following system of records:

**ALTERED SYSTEM OF RECORDS**

**18–05–17**

**SYSTEM NAME:**

Investigatory Material Compiled for Personnel Security, Suitability, Positive Identification Verification and Access Control for the Department of Education Security Tracking and Reporting System (EDSTAR).

**SECURITY CLASSIFICATION:**

None.

**SYSTEM LOCATIONS:**

(1) Security Services, Office of Management, U.S. Department of Education, 400 Maryland Avenue, SW., Washington, DC 20202–5345.

(2) U.S. Department of Education, Data Center, 6710 Oxon Hill Road, Oxon Hill, MD 20745–1117.

(3) U.S. Office of Personnel Management (OPM), Federal Investigations Processing Center, P.O. Box 618, 1137 Branchton Road, Boyers, PA 16018–0618.

(4) Verisign, 487 E. Middlefield Road, Mountain View, CA 94043–4047.

(5) U.S. Department of Justice (DOJ), DOJ Rockville Data Center, 1151–D Seven Locks Road, Rockville, MD 20854–0001.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

This system contains information on applicants seeking Federal or contract employment with the Department, current Federal employees and contractors, and other persons or entities doing business with the Department, or persons either seeking unescorted access to the facilities, or access to the information systems of the Department, or both. The system does not cover term employees of less than 30 calendar days with monitored access to either the Department's facilities or information system, or both. Nor does it cover occasional visitors or short-term guests to the Department to the extent that they are issued non-Personal Identity Verification (PIV) temporary identification.

**CATEGORIES OF RECORDS IN THE SYSTEM:**

This system consists of records containing investigative information pertaining to current and former Department employees, current and former contractor personnel, and current employees of entities making offers to the Department for purposes of doing business. This information may include information pertaining to the individuals' character, conduct, and loyalty to the United States as relevant to determination of their suitability for employment in the Department. This system of records may include an individual's name, former names, birth date, birth place, Social Security number, home address, phone numbers, employment history, residential history, education and degrees earned, names of associates and references and their contact information, citizenship, names of relatives, birth dates and birth places of relatives, citizenship of relatives, names of relatives who work for the Federal government, mental health history, drug use, financial information, summary report of investigation, results of suitability decisions, level of security clearance, date of issuance of security clearance, requests for appeal, witness statements, investigator's notes, tax return information, credit reports, security violations, circumstances of violation, and agency action taken.

These records also may, as appropriate to the individual being investigated, include the following types of information:

(1) Documentation as to his or her arrests and convictions for violations of the law.

(2) Reporting as to interviews held with the individual, his or her present and former supervisors, co-workers, associates, neighbors, educators, etc.

(3) Correspondence relating to adjudication matters involving the individual.

(4) Reports of inquiries made of law enforcement agencies for information about the individual contained in the agencies' records.

(5) Information provided by organizations having association with the individual, such as employers, educational institutions attended, professional or fraternal or social organizations to which the individual is or was a member, etc.

(6) Reports of action following an OPM investigation or a Federal Bureau of Investigation Section 8(d) full field investigation.

(7) Personal access logs of individuals entering access controlled space.

(8) Public Key Infrastructure (PKI) Certificates issued under direct guidance from Homeland Security

Presidential Directive (HSPD)–12 and Federal Information Processing Standard (FIPS)–201.

(9) Personal fingerprint records for identification and criminal records checks.

(10) Other information developed from the previous sources.

In addition, this system contains records maintained on individuals issued PIV credentials by the Department. These records may include the following data fields: Full name; Social Security number; date of birth; signature; image (photograph); fingerprints; hair color; eye color; height; weight; organization or office of assignment; company name; copy of background investigation form; PIV card issuance and expiration dates; personal identification number (PIN); results of background investigation; PIV request form; PIV registrar approval signature; PIV card serial number; emergency responder designation (if applicable); copies of documents used to verify identification or information derived from those documents such as document title, document issuing authority, document number, document expiration date, document other information); level of national security clearance and expiration date; computer system user name; user access and permission rights, authentication certificates; and digital signature information. For those issued non-PIV identification these fields do not apply.

**Note 1:** OPM and DOJ issue the standard forms used to collect information in this system, i.e. Standard Form (SF) 85, SF–85P, SF–85PS, SF–86, SF–87, and Fingerprint card FD–258.

**Note 2:** To the extent that the Department has records of a personnel investigative nature that come from OPM or its contractors, these records are covered by OPM/CENTRAL–9, Personnel Investigations Records, and are not covered by this system notice.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

HSPD–12, Policy for a Common Identification Standard for Federal Employees and Contractors (August 27, 2004); Executive Orders 10450, 18 FR 2489, 3 CFR 1949–1953 Comp., p. 936); 10577 (3 CFR 1954–1958 Comp., p. 218); and 12968 (Access to Classified Information); 5 U.S.C. 3301 and 7301; Federal Property and Administrative Act of 1949, as amended through Public Law 106–580; and 5 CFR parts 5, 731, 732, and 736.

**PURPOSE(S):**

Records in this system are maintained to assist in making determinations concerning suitability for Federal employment, security clearances, access to classified information, unescorted access to Federal government owned and Federal government leased facilities or restricted areas, and evaluations as to acceptability for performance under Federal contracts or other agreements with the Federal government. Purposes of this system also include: Ensuring the safety and security of Federal facilities, systems, and information resources, as well as the safety and security of the occupants and users of these facilities, systems, and information resources; verifying that persons entering Federal facilities and using Federal systems and information resources, are authorized to do so; and tracking and controlling PIV cards issued to persons entering the Federal government's facilities and using its systems and information resources.

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:**

The Department may disclose information contained in a record in this system of records under the routine uses listed in this system of records without the consent of the individual if the disclosure is compatible with the purposes for which the record was collected. The Department may make these disclosures on a case-by-case basis or, if the Department has complied with the computer matching requirements of the Computer Matching and Privacy Protection Act of 1998, as amended, under a computer matching agreement.

(1) *Program Purpose.* The Department may disclose records from this system of records to any source or potential source from which information is requested in the course of an investigation concerning the suitability or retention of an employee or a contractor, or the retention of a security clearance, contract, grant, license, or other benefit, to the extent necessary to identify the individual being investigated, inform the source of the nature and purpose of the investigation, and to identify the type of information requested.

(2) *Enforcement Disclosure.* The Department may disclose relevant records to a Federal, State, local, foreign, or tribal entity or other public authority responsible for the investigation, prosecution, enforcement, or implementation of a statute, rule, regulation, or order, when a record on its face or in combination with any other information indicates a violation or potential violation of law (whether civil, criminal, or regulatory in nature) if that information is relevant to any enforcement, regulatory, investigative, or prosecutorial responsibility of the receiving entity. It is Office of Management policy not to disclose records under this routine use that pertain to those questions for which the Office of Management has promised confidentiality under SF–85P, Questionnaire for Public Trust Positions.

(3) *Contract Disclosure.* If the Department contracts with an entity for the purpose of performing any function that requires disclosure of records in this system to employees of the contractor, the Department may disclose the records as a routine use to those employees. Before entering into such a contract, the Department shall require the contractor to maintain Privacy Act safeguards as required under 5 U.S.C. 552a(m) with respect to the records in the system.

(4) *Litigation or Alternative Dispute Resolution (ADR) Disclosure.* (a) *Introduction.* In the event that one of the following parties is involved in litigation or ADR, or has an interest in litigation or ADR, the Department may disclose certain records to the parties described in paragraphs (b), (c), and (d) of this routine use under the conditions specified in those paragraphs:

(i) The Department or any of its components.

(ii) Any Department employee in his or her official capacity.

(iii) Any employee of the Department in his or her individual capacity where the DOJ has agreed to or has been requested to provide or arrange for representation of the employee.

(iv) Any employee of the Department in his or her individual capacity where the Department has agreed to represent the employee.

(v) The United States where the Department determines that the litigation is likely to affect the Department or any of its components.

(b) *Disclosure to the DOJ.* If the Department determines that disclosure of certain records to the DOJ or attorneys engaged by DOJ is relevant and necessary to litigation or ADR and is compatible with the purpose for which the records were collected, the Department may disclose those records as a routine use to DOJ.

(c) *Adjudicative Disclosure.* If the Department determines that disclosure of certain records to an adjudicative body before which the Department is authorized to appear or to an individual or entity designated by the Department or otherwise empowered to resolve or mediate disputes is relevant and necessary to litigation or ADR and is compatible with the purpose for which the records were collected, the Department may disclose those records

as a routine use to the adjudicative body, individual, or entity.

(d) *Disclosure to Parties, Counsel, Representative, or Witnesses.* If the Department determines that disclosure of certain records to a party, an opposing counsel, representative, or witness is relevant and necessary to litigation or ADR and is compatible with the purpose for which the records were collected, the Department may disclose those records as a routine use to a party, counsel, representative, or witness.

(5) *Freedom of Information Act (FOIA) Advice Disclosure.* The Department may disclose information from this system of records to DOJ for the purpose of obtaining advice regarding the releasability of records maintained in this system of records under the FOIA and the Privacy Act of 1974.

(6) *Congressional Member Disclosure.* The Department may disclose information from this system of records to a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained.

(7) *Disclosure for Use by Other Law Enforcement Agencies.* The Department may disclose information from this system of records to any Federal, State, local or foreign agency or other public authority responsible for enforcing, investigating, or prosecuting violations of administrative, civil, or criminal law or regulation if that information is relevant to any enforcement, investigative, or prosecutorial responsibility within the receiving entity's jurisdiction.

(8) *Disclosure for Use for Intelligence Activities.* The Department may disclose information from this system of records to Federal, State, or local agencies, other appropriate entities or individuals, or, through established liaison channels, to selected foreign governments, in order to enable an intelligence agency to carry out its responsibilities as authorized by law, including the National Security Act of 1947 as amended, the CIA Act of 1949 as amended, Executive Order 12333 or any successor order, applicable national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders or directives.

(9) *Employment, Benefits, and Contracting Disclosure.* (a) *For Decisions by the Department.* The Department may disclose information from this system of records to a Federal, State, or local agency or to another public authority or professional organization, to obtain information relevant to the Department's conduct of a security or suitability investigation of an individual seeking employment, licensure, other benefits, or to perform contractual services for, or to otherwise associate with, the Department.

(b) *For Decisions by Other Public Agencies and Professional Organizations.* The Department may disclose information from this system of records to a Federal, State, local, or foreign agency, or other public authority or professional organization, so that the receiving entity may obtain information relevant to its conduct of a security or suitability investigation of an individual seeking employment, licensure, other benefits, or to perform contractual services for, or to otherwise associate with, the receiving entity.

(10) *Employee Grievance, Complaint, or Conduct Disclosure.* If a record is relevant and necessary to a grievance, complaint, or disciplinary proceeding regarding a present or former employee of the Department, the Department may disclose the record in the course of an investigation, fact-finding, or adjudication to another agency of the Federal government, or to any witness, designated fact-finder, mediator, or other person designated to resolve issues or decide the matter. The disclosure may only be made during the course of the investigation or the proceeding.

(11) *Disclosure in the Course of Responding to Breach of Data.* The Department may disclose records to appropriate agencies, entities, and persons when (a) it is suspected or confirmed that the security or confidentiality of information in this system has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or by another agency or entity) that rely upon the compromised information; and (c) the disclosure is made to such agencies, entities, and persons who are reasonably necessary to assist the Department in responding to the suspected or confirmed compromise and in helping the Department prevent, minimize, or remedy such harm.

(12) *Disclosure to Protect Safety and Security of Department Employees, Customers, and Facilities.* The Department may disclose to Federal, State, and local law enforcement agencies and private security contractors, as appropriate, information that the Department deems necessary in order to: (a) Assist with the protection of the safety of Department employees and customers, the security of the Department's workplace, or the operation of the Department's facilities or information systems; or (b) assist with investigations or prosecutions with respect to activities that affect such safety and security or activities that disrupt the operation of the Department.

**Note 3:** Disclosures within the Department of data pertaining to date and time of entry and exit of a Department employee working in the District of Columbia may not be made to supervisors, managers, or any other persons (other than the individual to whom the information applies) to verify employee time and attendance records for personnel actions because 5 U.S.C. 6106 prohibits Federal Executive agencies (other than the Bureau of Engraving and Printing) from using a recording clock within the District of Columbia, unless used as a part of a flexible schedule or compressed work schedule under 5 U.S.C. 6120, *et seq.*

**POLICIES AND PRACTICES OF STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:**

**STORAGE:**

Records are maintained on paper and in electronic form. Paper records are stored in fire resistant locked file cabinets in locked access-controlled rooms. Within the locked access-controlled room, electronic files are encrypted and stored in alarmed electronic retrieval file systems. The data servers, the laptops, and the desk computers where the data resides are in locked access-controlled rooms.

PIV identification card data on cardholders entering the Department's facilities is stored in an encrypted database.

**RETRIEVABILITY:**

Electronic and paper records are retrieved by an unique identifying number by the Department pursuant to the National Institute of Standards and Technology (NIST), Federal Information Processing Standard (FIPS) 201, Personal Identity Verification for Federal Employees and Contractors; this number is cross-referenced to the name of the individual.

**SAFEGUARDS:**

All physical access to the Department's sites, and the sites of the Department's contractors where this system of records is maintained, is controlled and monitored by security personnel who check each individual entering the building for his or her employee or visitor badge.

In accordance with the Department's Administrative Communications System (ACS) Directive OM: 5–101 entitled

''Contractor Employee Personnel Security Screenings,'' all contract and Department personnel who have facility access and system access are required to undergo a security clearance investigation. Individuals requiring access to Privacy Act data are required to hold, at a minimum, a moderate-risk security clearance level. These individuals are required to undergo periodic screening at five-year intervals.

In addition to undergoing a security clearance investigation, contract and Department personnel are required to complete security awareness training on an annual basis. This training is required to ensure that contract and Department users are trained appropriately in safeguarding Privacy Act data in accordance with OMB Circular No. A–130, Appendix III.

Computer databases are kept on encrypted servers on an isolated virtual local area network (V–LAN) that is not connected to any outside network including the Internet. Database accessibility is restricted to hard wire network connection from within the Office Management, Security Services, and direct Integrated Services Digital Network (ISDN) line to the Department of Justice (DOJ), or via secure portal to the Office of Personnel Management (OPM). Authorized log-on codes and passwords prevent unauthorized users from gaining access to data and system resources. All users have unique log-on codes and passwords. The password scheme requires that users must change passwords every 60 days and may not repeat the old password.

Any individual attempting to log on who fails is locked out of the system after three attempts. Access after that time requires intervention by the system manager.

**RETENTION AND DISPOSAL:**

Most background investigative records are maintained in accordance with General Records Schedule (GRS) 18, Item 22—destroy not later than five years after separation or transfer of employee or no later than five years after contract relationship expires, whichever is later. Records are destroyed by deletion or shredding.

Reports of background investigations conducted by the Office of Inspector General under delegated authority of the OPM are retained in accordance with OPM retention standards for similar records, pending National Archives and Records Administration (NARA) approval. Records will be maintained for 15 years after the last investigative activity, except investigations involving potentially actionable issue(s) will be maintained for 25 years after the last investigative activity and then destroyed by deletion or shredding.

Personal access logs of individuals entering controlled space are retained in accordance with GRS 18, Item 17. In the Department's secured facilities, records are destroyed five years after final entry or five years after date of document, as appropriate. For all other facilities, records are destroyed two years after final entry or two years after date of document, as appropriate. Records are destroyed by deletion or shredding.

PKI certificates and PIV cards issued under guidance of HSPD–12 and FIPS–201 will be retained in accordance with the pending GRS disposition authority as issued by NARA, or in a NARA-approved, Departmental records retention schedule, as appropriate.

**SYSTEM MANAGER(S) AND ADDRESS:**

Security Services, Office of Management, U.S. Department of Education, 400 Maryland Avenue, SW., Room 2W314, Washington, DC 20202–5345.

**NOTIFICATION PROCEDURE:**

If an individual wishes to determine whether a record exists regarding him or her in this system of records, the individual must contact the system manager and provide his or her name, date of birth, social security number, signature, and the address to which the record information should be sent. This information is required to ensure the positive identification of the person's record in the system. Requests for notification about an individual must meet the requirements of the regulations in 34 CFR 5b.5.

**RECORD ACCESS PROCEDURE:**

If an individual wishes to gain access to a record in this system, he or she must contact the system manager and provide information as described in the notification procedure.

**CONTESTING RECORD PROCEDURE:**

If an individual wishes to change the content of a record in the system of records, he or she must contact the system manager with the information described in the notification procedure, identify the specific item or items to be changed, and provide a written justification for the change, including any supporting documentation. Requests to amend a record must meet the requirements of the regulations in 34 CFR 5b.7.

**RECORD SOURCE CATEGORIES:**

Information contained in this system of records is obtained from—

(a) Investigative and other record material furnished by other Federal entities, other departmental components, State, local, and foreign governments;

(b) Applications and other personnel and security forms;

(c) Personal investigation, written inquiry, interview, and the electronic accessing of computer databases of sources, such as the OPM system of records known as Personnel Investigations Records (OPM/Central-9), employers, educational institutions, references, neighbors, associates, police departments, courts, credit bureaus, medical records, probation officials, prison officials, DOJ, newspapers, magazines, periodicals, and other publications; and

(d) Confidential sources.

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**

The Secretary has exempted by regulation—in 34 CFR 5b.11(d)—this system of records only to the extent that the information is investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access to classified information from the following provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k)(5):

(1) 5 U.S.C. 552a(c)(3), regarding access to an accounting of disclosures of records.

(2) 5 U.S.C. 552a(d)(1) through (4) and (f), regarding notification of and access to records and correction or amendment of records.

(3) 5 U.S.C. 552a(e)(4)(G) and (H) regarding inclusion of information in the system notice about procedures for notification, access, and correction of records.

As indicated in 34 CFR 5b.11(f), individuals will be provided access to information in this system, except when, in accordance with the provisions of 5 U.S.C. 552a(k)(5):

(1) The disclosure of such information would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence; or

(2) The information was obtained prior to September 28, 1975 and the disclosure of such information would reveal the identity of the source under an implied promise that the identity of the source would be held in confidence.

[FR Doc. E7–23059 Filed 11–26–07; 8:45 am]

**BILLING CODE 4000–01–P**