Privacy Impact Assessment
for the

EDSTAR System (OM)

Date
September 2007

Contact Point
System Owner: Director of Security Services, OM

U.S. Department of Education

1. **What information will be collected for the system (e.g., name, Social Security number, annual income, etc)?**

The Investigatory Material Compiled for Personnel Security, Suitability, Positive Identification Verification and Access Control for the Department of Education Security Tracking and Reporting System (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, government-wide standard for secure and reliable forms of Personal Identity Verification (PIV).

This system contains information on applicants seeking Federal or contract employment with the Department, current and former Federal employees and contractors, and other persons or entities doing business with 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.

The information contained in the System 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, as well as 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 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:

- Documentation as to his or her arrests and convictions for violations of the law.
- Reporting as to interviews held with the individual, his or her present and former supervisors, co-workers, associates, neighbors, educators, etc.
- Correspondence relating to adjudication matters involving the individual.
- Reports of inquiries made of law enforcement agencies for information about the individual contained in the agencies records.

- 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.
- Reports of action following an OPM investigation or a Federal Bureau of Investigation Section 8(d) full field investigation.
- Personal access logs of individuals entering access controlled space.
- Public Key Infrastructure (PKI) Certificates issued under direct guidance from Homeland Security Presidential Directive (HSPD)-12 and Federal Information Processing Standard (FIPS)-201.
- Personal fingerprint records for identification and criminal records checks.
- 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

2. Why is this information being collected?

This information is being collected 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

3. How will the Department of Education use this information?

This information will be used to make 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.

4. Will this information be shared with any other entity? If so, with whom?

This information may be shared with other entities. 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.

OM may also disclose information in this system under the routine uses listed in the System of Record notice for EDSTAR 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. Disclosures may include:

- Enforcement Disclosure
- Contract Disclosure
- Litigation or Alternative Dispute Resolution (ADR) Disclosure
- Freedom of Information Act (FOIA) Advice Disclosure
- Congressional Member Disclosure
- Disclosure for Use by Other Law Enforcement Agencies
- Disclosure for Use for Intelligence Activities
- Employment, Benefits, and Contracting Disclosure
- Employee Grievance, Complaint, or Conduct Disclosure
- Disclosure in the Course of Responding to Breach of Data
- Disclosure to Protect Safety and Security of Department Employees, Customers, and Facilities

3. Describe the notice or opportunities for consent that would be/or are provided to individuals about what information is collected and how that information is shared with others organizations. (e.g., posted Privacy Notice)

In all cases, PIV applicants are provided notices required by the Privacy Act, 5 USC 552(a)(e)(3). The notice states the reasons for collecting information, the consequences of failing to provide the requested information, and explains how the information is used. The collection, maintenance, and disclosure of information complies with the Privacy Act and the published System of Records Notice (SORN) for the System. By signing the PIV application form, applicants acknowledge that the Department of Education may use their

information as outlined in the Privacy Act Statement and associated Privacy Act SORN. While there is no legal requirement to use a PIV Card, employees who do not use a PIV Card will be treated as visitors when entering a federal building and will be barred from access to certain federal resources. If using a PIV card is a condition of the job, withholding requested information will affect job placement or employment prospects.

4. How will the information be secured?

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.

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.

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. 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.

5. Is a system of records being created or updated with the collection of this information?

The System of Records Notice, "Investigatory Material Compiled for Personnel Security and Suitability Purposes" (18-05-17), currently exists, but is being amended and the system is being renamed to "Investigatory Material Compiled for Personnel Security, Suitability, Positive Identification Verification and Access Control for the Department of Education Security Tracking and Reporting System (EDSTAR)." The system of records titled Identification Media Records (18-05-16) will be deleted because it has been merged into and consolidated with the EDSTAR system of records.