Privacy Impact Assessment

For

Department of Education
Security Tracking and Reporting (EDSTAR) System

Date:
March 17, 2016

Point of Contact:
Woineshet Yirga-Keefe
Woineshet.Yirga-Keefe@ed.gov

System Owner:
Ronald Luczak
Ronald.Luczak@ed.gov

Authorizing Official:
Ronald Luczak
Ronald.Luczak@ed.gov

Author:
Brenda Daly
Brenda.Daly@ed.gov

Office of Management
U.S. Department of Education
1. **System Information.** Describe the system - include system name, system acronym, and a description of the system, to include scope, purpose and major functions. Indicate whether the system is new or existing, and whether or not the PIA is new or being updated from a previous version; specify whether the system is ‘agency’ or ‘contractor.

The U.S. Department of Education Security Tracking and Reporting System (EDSTAR) is designed to implement the requirements of Homeland Security Presidential Directive 12 (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 the Department and seeking unescorted access to the facilities, or accessing Departmental information systems, or both. The systems also complies investigatory material for Personnel Security, Suitability, Positive Identification Verification and Access Control. The system does not cover short term employees or contractors of less than 30 calendar days with monitored access to either the Department’s facilities or information system, or both. It also does not cover occasional visitors or short-term guests to the Department to the extent that they are issued temporary identification cards (non-PIV ID).

This PIA is an updated version that supersedes the September 2007 version. EDSTAR is a Departmental System.

2. **Legal Authority.** Cite the legal authority to collect and use this data. What specific legal authorities, arrangements, and/or agreements regulate the collection of information?

   - 5 CFR 731 (Suitability)
   - 5 CFR 732 (National Security)
   - 5 CFR 736 (Personnel Investigations)
   - Executive Order 10450
   - Executive Order 9397

3. **Characterization of the Information.** What elements of personally identifiable information (PII) are collected and maintained by the system (e.g., name, social security number, date of birth, address, phone number)? What are the sources of information (e.g., student, teacher, employee, university)? How is the information collected (website, paper form, on-line form)? Is the information used to link or cross-reference multiple databases?

The information contained in the System may include information pertaining to individuals' character, conduct, and loyalty to the United States as relevant to the 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 on interviews held with the individual, his or her present and former supervisors, coworkers, 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.

This information is gathered directly from the person to whom the information pertains and from other people with information about the person. It also comes from databases, websites, and various available records about the person being investigated.

4. **Why is the information collected?** *How is this information necessary to the mission of the program, or contributes to a necessary agency activity?* Given the amount and any type of data collected, discuss the privacy risks (internally and/or externally) identified and how they were mitigated.

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. The purpose of this system also includes 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.

In an effort to reduce privacy risks, the following mitigation steps are in place:

- Associates who has a job-related need-to-know require a username and password before access can be granted.
- System access is assigned based on job function requirements and are maintained through permissions based access controls.
- Associates are required to complete the Security Awareness Training annually.
- Access is only available through direct connection to the network or VPN connectivity and is not externally available.

5. **Social Security Number (SSN).** *If an SSN is collected and used, describe the purpose of the collection, the type of use, and any disclosures. Also specify any alternatives that you considered, and why the alternative was not selected. If system collects SSN, the PIA will require a signature by the Assistant Secretary. If no SSN is collected, no signature is required.*

The system collects and maintains SSN on all individuals. SSNs are obtained as a way of ensuring the identity of an individual during the course of investigations. The SSN uniquely identifies individuals ensuring timely investigations and adjudications. There is no viable alternative to collecting the SSN for identification purposes.
The SSN is disclosed internally within the Department for investigative purposes, and is shared with other Federal agencies. The SSN are used to determine what clearances/investigations exist on individuals or other relevant information available from another Federal agency. The SSN is disclosed and exchanged with state/local government to gather investigative data and records.

6. **Uses of the Information.** What is the intended use of the information? How will the information be used? Describe all internal and/or external uses of the information. What types of methods are used to analyze the data? Explain how the information is used, if the system uses commercial information, publicly available information, or information from other Federal agency databases.

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. Methods used to analyze information include an adjudicator’s ability identify character traits and conduct sufficient to determine whether an individual is likely or not likely to be able to carry out the duties of a Federal job with appropriate integrity, efficiency, and effectiveness. All information from public sources, commercial sources or other governmental agencies is acquired to aid the adjudicator in making a determination.

7. **Internal Sharing and Disclosure.** With which internal ED organizations will the information be shared? What information is shared? For what purpose is the information shared?

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.

8. **External Sharing and Disclosure.** With what external entity will the information be shared (e.g., another agency for a specified programmatic purpose)? What information is shared? For what purpose is the information shared? How is the information shared outside of the Department? Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding or other type of approved sharing agreement with another agency?

This information may be shared with external 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. The information can also be disclosed for investigative purposes and for reporting required information to other government agencies.

OM may also disclose information in this system under the routine user 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.

9. Notice. Is notice provided to the individual prior to collection of their information (e.g., a posted Privacy Notice)? What opportunities do individuals have to decline to provide information (where providing the information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent?

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. This notice is included on the PIV enrollment form and is available on the Department’s intranet. 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.

Additional privacy notices are included on the forms required to be completed as part of the background investigation process, specifically the Questionnaire for National Security Positions, the Questionnaire for Public Trust Positions, and the Questionnaire for Non-Sensitive Positions.

10. Web Addresses. List the web addresses (known or planned) that have a PrivacyNotice.

There will be no public facing web address for this system; therefore a privacy notice is not required.

11. Security. What administrative, technical, and physical security safeguards are in place to protect the PII? Examples include: monitoring, auditing, authentication, firewalls, etc. Has a C&A been completed? Is the system compliant with any federal security requirements?

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 background investigation. Individuals requiring access to significant Privacy Act data are required to hold, at a minimum, a Public Trust Moderate Risk access level. These individuals are required to undergo periodic screenings. In
addition to undergoing a background 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. The system has had a C&A completed and is compliant with federal information security requirements.

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.

12. **Privacy Act System of Records.** Is the information within the system retrieved by personal identifier? Is a system of records being created or altered under the Privacy Act, 5 U.S.C. 552a? Is this a Department-wide or Federal Government-wide SORN? If a SORN already exists, what is the SORN Number?


13. **Records Retention and Disposition.** Is there a records retention and disposition schedule approved by the National Archives and Records Administration (NARA) for the records created by the system development lifecycle AND for the data collected? If yes – provide records schedule number:

Records are maintained and disposed of in accordance with NARA’s General Records Schedules 18, Security and Protective Services Records.