Privacy Impact Assessment (PIA)
for the

Education Security Tracking and Reporting System (EDSTAR)

May 6, 2020

For PIA Certification Updates Only: This PIA was reviewed on [Enter date] by [Name of reviewer] certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Lisa Senecal
Contact Email: Lisa.Senecal@ed.gov

System Owner

Name/Title: Chris Shanefelter
Principal Office: Office of Finance and Operations

Please submit completed Privacy Impact Assessments to the Privacy Office at privacysafeguards@ed.gov
1. Introduction

1.1. Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

The Department of Education’s Security Tracking and Reporting System (EDSTAR) system is a background investigation, security clearance, Personal Identity Verification (PIV) ID issuance and physical access control and monitoring tracking system consisting of a group of four applications that reside on the Department of Education’s network. The application includes WEBS for fingerprint and PII storage, MyID for PIV card credentials, SecurityManager for background investigations and security clearance tracking, and DSX for managing the physical security of the Department of Education buildings. The EDSTAR System supports the Office of Finance and Operations and the Security Services within that Principal Office to create, process and track security records, issue PIV IDs, control physical access and monitor security mechanisms for all Department employees and contractors.

1.2. Describe the purpose for which the personally identifiable information (PII) is collected, used, maintained or shared.

The purpose for which PII is maintained in EDSTAR is to enable the Security staff to store and manage ED personnel security information, issue PIV Identification cards and to provide physical access to the Department’s buildings and office locations.

1.3. Is this a new system, or one that is currently in operation?

Currently Operating System

1.4. Is this PIA new, or is it updating a previous version?

Updated PIA

---

1 The term “personally identifiable information” refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. OMB Circular A-130, page 33
1.5. Is the system operated by the agency or by a contractor?

Agency

1.5.1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

☑ N/A

Click here to select.

2. Legal Authorities and Other Requirements

If you are unsure of your legal authority, please contact your program attorney.

2.1. What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system? Please include name and citation of the authority.

- 5 CFR 731 (Suitability)
- 5 CFR 732 (National Security)
- 5 CFR 736 (Personnel Investigations)
- Executive Order 13467: Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information
- Executive Order 9397: NUMBERING SYSTEM FOR FEDERAL ACCOUNTS RELATING TO INDIVIDUAL PERSONS
- Executive Order 13526: Classified National Security Information
- Executive Order 10577: Amending the Civil Service Rules and authorizing a new appointment system for the competitive service
- Executive Order 10865: Safeguarding classified information within industry
- Executive Order 12333: United States intelligence activities

SORN

2.2. Is the information in this system retrieved by an individual’s name or personal identifier such as a Social Security Number or other identification?

Yes
2.2.1. If the above answer is **YES**, this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).\(^2\) Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

☐ N/A


2.2.2. If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

✓ N/A

Click here to enter text.

**Records Management**

If you do not know your records schedule, please consult with your records liaison or send an email to [RMHelp@ed.gov](mailto:RMHelp@ed.gov)

2.3. What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

The Records disposition schedules are:

- Disposition Authority Number: GRS-2017-0006-0024, Records of people not issued clearances. Disposition: Temporary, destroy 1 year after consideration of the candidate ends, but longer retention is authorized if required for business use.
- Disposition Authority Number: DAA-GRS-2017-0006-0025, Records of people issued clearances. Disposition: Temporary, Destroy in accordance with delegated authority agreement or memorandum of understanding.

\(^2\) A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. [https://connected.ed.gov/om/Documents/SORN-Process.pdf](https://connected.ed.gov/om/Documents/SORN-Process.pdf)
2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

Yes

3. Characterization and Use of Information

Collection

3.1. List the specific PII elements (e.g., name, email, address, phone number, date of birth, Social Security, etc.) that the system collects, uses, disseminates, or maintains.

Full name, place and date of birth, Social Security number (SSN), citizenship status, phone number, fingerprints, copies of proofs of identification, Department organizational information (pay grade, position designation level, office, work location, etc.), security clearance level and credential data (LAN ID, badge information, certificates, unique credential identifiers).

Information collected as part of a background investigation conducted by the Office of Personnel Management (OPM) which may include educational information, financial information, criminal history and other legal information, medical information, employment history, and residential history. For more information please reference the Electronic Questionnaire for Investigations Processing (eQIP) Privacy Impact Assessment at: https://www.opm.gov/information-management/privacy-policy/privacy-policy/e-qip.pdf

EDSTAR may also maintain documents related to the adjudication of an employee or contractor’s background investigation.

3.2. Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2?

Yes

3.3. What are the sources of PII collected (e.g., individual, school, another agency, commercial sources, etc.)?

The main source of information maintained in EDSTAR is the Defense Counterintelligence and Security Agency (DCSA) which is responsible for initially collecting PII for the purposes of conducting background investigations. In the event the Department collects additional PII (for example, in issuing a PIV card or requesting
3.4. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, web page, database, etc.)?

Information from DCSA is shared electronically with the Department. In the event the Department collects additional PII from an individual, it is either on a paper or electronic form.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected? Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

Throughout the individual’s clearance process the Security Office validates the PII information through various methods such as conducting a fingerprint check, credit history check, requesting a background investigation and other investigations as deemed necessary based on suitability or national security investigation requirements.

Initial validation of PII collected through the background investigation process is the responsibility of DCSA but once an investigation concludes and the results are shared with the Department, the Security Services office may further validate the data.

Continuous validation comes from comparing employee data against the information received from the National Business Center.

3.6. Describe how the PII is used to achieve the purpose stated in Question 1.2 above.

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, facilitate the issuance of PIV and identification media, and access to restricted areas.

3.7. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

3 Examples include restricted form filling, account verification, editing and validating information as it’s collected, and communication with the individual whose information it is.
3.7.1. If the above answer is YES, what controls are in place to minimize the risk and protect the data?

☑ N/A

Click here to enter text.

Social Security Numbers

*It is the Department’s Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.*

3.8. Does the system collect Social Security Numbers? Note that if the system maintains Social Security Numbers but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

Yes

3.8.1. If the above answer is YES, explain the purpose for its collection, and how the SSN will be used.

☐ N/A

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 is disclosed internally within the Department for investigative purposes and is shared with other Federal agencies listed in Question 5.5. The SSN is 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.

3.8.2. Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

☐ N/A

There were no alternatives considered. SSN’s are required for the purposes of the investigations.

4. Notice

4.1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? If notice is not provided, explain why not.
A Privacy Act statement is provided on all paper and electronic forms requesting PII, such as the applications for fingerprinting and an identification card. The system provides public notice by the publishing of a SORN and PIA.

4.2. Provide the text of the notice or the link to the webpage where the notice is posted if notice is provided other than by SORN or PIA.

☐ N/A

 Department of Education (ED) is authorized to ask for the information requested on this form by Homeland Security Presidential Directive (HSPD)-12, and 31 USC 7701. The information and biometrics collected as part of the Federal identity-proofing program under HSPD-12 are used to verify the personal identity of ED applicants for employment, employees, contractors, and affiliates (such as students or interns) prior to issuing a Department identification credential. The credentials are used to authenticate electronic access requests from ED employees, contractors, and affiliates issued a Department identification credential to gain access to ED facilities and networks (where available) through digital access control systems, as well as to other federal government agency facilities and systems where permitted by law. The information collected on this form is protected by the Privacy Act, 5 USC Section 552(a) and maintained under the authority of 38 USC Section 501 and 38 USC Sections 901-905 in ED system of records.

The Privacy Act (5 U.S.C. § 552a(b)) permits ED to disclose the information you provide on this form in accordance with published routine uses, which include but are not limited to the following: civil or criminal law enforcement, constituent congressional communications initiated at your request, litigation or administrative proceedings, administration of the program, including verification of identity and status, personnel administration by Federal agencies. to contractors performing agency functions, FOIA administration, intelligence activities, employment, benefits, and contracting disclosure, employee grievance, complaint, or conduct, responding to breach of data, safety and security of Department employees, customers, and facilities.

4.3. What opportunities are available for individuals to consent to uses (including new uses of previously collected PII), decline to provide PII, or opt out of the project?

EDSTAR processes individuals for security approval to work within the Department of Education and access the Department’s facilities and information systems. Individuals may opt to not provide information; however, if the information is not provided, they will not meet the suitability requirements and will be ineligible for employment at the Department or access to its facilities.
4.4. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practice, policy, or activities that affect the PII and privacy to ensure that individuals are aware of and can consent to, where feasible, these changes?

Yes

5. Information Sharing and Disclosures

Internal
5.1. Will PII be shared internally with other ED principal offices? If the answer is NO, please skip to Question 5.4.

Yes

5.2. What PII will be shared and with whom?

☐ N/A

PII is not explicitly shared with other principal offices however Contracting Office Representatives (CORs) and Information System Security Officers (ISSO)s from other principal offices will have access to EDSTAR’s Security Manager to verify information such as investigation or clearance level. PII accessed will include basic identifier information.

5.3. What is the purpose for sharing the specified PII with the specified internal organizations?

☐ N/A

The information is accessible to appropriate personnel that require access to the information to verify investigation or clearance level to determine access eligibility to information systems and Department locations.

External
5.4. Will the PII contained in the system be shared with external entities (e.g. another agency, school district, the public, etc.)? If the answer is NO, please skip to Question 6.1.

Yes
5.5. What PII will be shared and with whom? List programmatic disclosures only.\(^4\)

Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☐ N/A

Individual’s name, former names, birth date, birthplace, Social Security number, home address, phone numbers are shared is shared with DCSA and fingerprints are submitted to Department of Justice (DOJ).

5.6. What is the purpose for sharing the PII with the specified external entities?

☐ N/A

PII is shared with DCSA and DOJ to initiate background investigations

5.7. Is the sharing with the external entities authorized?

☐ N/A

Yes

5.8. Is the system able to provide and retain an account of any disclosures made and make it available upon request?

☐ N/A

Yes

5.9. How is the PII shared with the external entity (e.g. email, computer match, encrypted line, etc.)?

☐ N/A

PII is shared via interconnections EDSTAR has with DOJ and DCSA. The information is shared with both using respective encrypted VPN-tunnel.

5.10. Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

☐ N/A

Yes

5.11. Does the project place limitation on re-disclosure?

☐ N/A

\(^4\) If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.
6. Redress

6.1. What are the procedures that allow individuals to access their own information?

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 provisions of the Privacy Act 5 U.S.C. 552a(d)(1) through (4) and (f), regarding notification of and access to records and correction or amendment of record pursuant to 5 U.S.C. 552a(k)(5).

6.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

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 provisions of the Privacy Act 5 U.S.C. 552a(d)(1) through (4) and (f), regarding notification of and access to records and correction or amendment of record pursuant to 5 U.S.C. 552a(k)(5).

6.3. How does the project notify individuals about the procedures for correcting their information?

Individuals are notified of this system’s exemption through the publication of this PIA, the SORN referenced in 2.2.1, and through the Department’s regulations at 34 CFR 5.

7. Safeguards

If you are unsure which safeguards will apply, please consult with your ISSO.

7.1. Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

Yes

7.2. Is an Authority to Operate (ATO) required?
7.3. Under NIST FIPS Pub. 199, what is the security categorization of the system: **Low, Moderate, or High?**

- N/A
- **Moderate**

7.4. What administrative, technical, and physical safeguards are in place to protect the information?

All security controls required to be implemented for a Moderate system containing PII have been implemented. All administrative, technical and physical security controls are documented in the System Security Plan (SSP).

Access to EDSTAR is only available to authenticated users utilizing two-factor authentication on the internal Department network who have a valid system user ID and have completed the Annual Cybersecurity and Privacy Awareness Training. The EDSTAR system owner approves all access and roles and responsibilities and ensures all users are provided a copy of the Rules of Behavior (ROB) which users must acknowledge and sign prior to receiving access to the system.

The boundaries of EDSTAR are protected by a combination of firewalls, intrusion detection system (IDS), and event monitoring system(s).

EDSTAR server(s) are housed in environmentally controlled server room(s). Access to production and reporting database by authorized users only. Strict instructions are provided to not extract or share PII data without proper handling and authorization.

Paper records are stored in fire resistant locked file cabinets in locked access-controlled rooms within a secured suite within a Department building.

7.5. Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?

- **Yes**

7.6. Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?
7.7. Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the security controls continue to work properly at safeguarding the PII.

EDSTAR undergoes annual system security authorization to maintain an active authority to operate (ATO). The ATO process includes an assessment of security and privacy controls, a plan of action and milestones to remediate any identified deficiencies, and a continuous monitoring program. Web scans, database scans, and penetration testing are conducted on the system based on established system schedule for scanning as part of testing and monitoring of the system. There are also scheduled system audits, end-user recertification/deprovisioning host and network intrusion detection, and vulnerability scan(s).

8. Auditing and Accountability

8.1. How does the system owner assess and ensure that the PII is used in accordance with stated practices in this PIA?

The System Owner periodically reviews information processing and maintains the access control list for who can read/write any PII information. The system owner also works directly with privacy office on privacy compliance documentation to ensure all information in this PIA is up to date and accurate. Ultimately, the EDSTAR system application(s) undergo yearly OMB Circular A-123 Appendix A (Management’s Responsibility for Enterprise Risk Management and Internal Control) assessment, and NIST 800-53 system security control self-assessments.

8.2. Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

8.3. What are the privacy risks associated with this system and how are those risks mitigated?

EDSTAR has several mitigation strategies in place such as the requirement for a Minimum T4 investigation, an active ED account, agreement of EDSTAR Rules of Behavior, accounts are individually approved by a system owner designee with role based accounts which limit the read/write capability along with audit capability. The main privacy risk identified is unauthorized access to the PII contained in EDSTAR. The risk(s) has been mitigated through privacy training for both contractor(s) and
Department Staff(s), restricting access to PII to those individuals with a direct business need for the information, and robust security related controls such as through the use of firewalls, intrusion detection systems, and event monitoring systems.