Privacy Impact Assessment (PIA)

for the

Education Security Tracking and Reporting System (EDSTAR)

March 26, 2024

Point of Contact

Contact Person: D'Mekka Thompson
Title: EDSTAR Alternate Information System Owner
Email: Dmekka.Thompson@ed.gov

System Owner

Name: Chris Shanefelter
Title: Information System Owner
Principal Office: Office of Finance and Operations

Submit completed Privacy Impact Assessments to the Privacy Office at
privacysafeguards@ed.gov

*Please complete this **Privacy Impact Assessment (PIA)**, which describes how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document.*
If a question does not apply to your system, answer with N/A.

- **Please ensure all responses are written in plain language. Write out all acronyms on first use and use acronyms consistently thereafter.**

- **For questions that are identical to those in the Privacy Threshold Analysis (PTA), please review the responses provided in the most recently approved PTA, determine whether the responses remain accurate, and, if so, use the same response in the PIA.**

1. Introduction

1.1. Describe the project or program that uses this information technology (IT) system, including the purpose of the project or program.

The U.S. Department of Education (Department) Security Tracking and Reporting System (EDSTAR) is a background investigation, security clearance, physical access control, and monitoring tracking system consisting of a group of four applications that reside on the Department's Enterprise Technology Services Integrated Service System (ETS-ISS) and Enterprise Technology Services-Infrastructure-Government Service System Information System (ETS-INFRA-GSS) general support systems. EDSTAR supports all principal offices at the Department to create, process, and track security records, control physical access, and monitor security mechanisms for all Department employees and contractors.

The implementation and deployment of EDSTAR is driven by Homeland Security Presidential Directive 12 (HSPD-12), which requires a Federal Government-wide standard for secure and reliable forms of identification issued to Federal employees and contractors. EDSTAR ensures Departmental compliance with all mandated credentialing requirements. EDSTAR also ensures timely delivery and processing of background investigations and adjudications for Department employees and contractors. EDSTAR consists of 4 components: bio-metric data, card management (Public Key Infrastructure/Key Management Infrastructure certificates), access control, and background investigation processing.

1.2. How does the IT system function to support the project or program as described in Question 1.1?

EDSTAR includes four applications:

- **WEBS (HID):** WEBS collects employee and contractor fingerprint and personal data including height, weight, date of birth, name, Social Security number (SSN),

place of birth, country of citizenship, gender, race, eye color, and hair color. This information is collected at an ID or security office. ID office and security personnel are the only users of WEBS. For onboarding employees and contractors, WEBS interfaces with the U.S. Department of Justice (DOJ) Civilian Applicant System (CAS) if a background check is not required (example: painters). If a background check is required, information is transmitted to the Defense Counterintelligence and Security Agency (DCSA) for criminal history checks. If necessary, DCSA may also share this information with State/local law enforcement entities as part of this process. All information listed in the first sentence of this paragraph is transmitted to DOJ and DCSA for their respective checks.

- **MyID (Intercede):** MyID is a retired card management system that stores employee/contractor credential information. While MyID previously created PIV cards, this component has been replaced by a new card management system, USAccess, that is not part of EDSTAR. MyID currently stores key certificates generated when MyID was the primary PIV card management system to recover and reissue the certificates if necessary. Certificates will be maintained in MyID for the duration of the NARA retention period.
- **Security Manager (Centech):** Security Manager is the background investigation and security clearance approval, tracking, and reporting application for EDSTAR. Information on background investigations is imported into Security Manager from two external applications maintained by DCSA: eDelivery and the Personnel Investigations Processing System (PIPS). This information is matched to case files for employees and prospective employees undergoing investigation. Each person with a case file in Security Manager is assigned a unique identifier that is used to track and retrieve information. Security Manager will automatically create a case file if there is not one in place. Once this information is transferred to Security Manager, Department personnel with appropriate roles can view the updated case files and make adjudicative decisions on background investigations.
- **DSX (DSX):** The DSX application is the current physical access control component for the Department. DSX controls automated access to designated Department buildings and includes closed-circuit TV cameras and associated monitors. DSX communicates with Department facility card readers via XML to ensure access is granted based on the access privileges associated with an individual's PIV card.

1.3. What are the technical elements and/or components of the IT system? Mark all that apply.

☒ Website	☐ Portal	☒ Application
☒ Database	☒ Server	☐ Other (Specify Below)

If you have been directed to "specify below," describe the type of technical elements and/or component:

1.4. Describe the purpose for which the personally identifiable information (PII)[1] is created, collected, used, processed, stored, maintained, disseminated, or disclosed by the IT system. If there is more than one type of individual from whom PII is collected (e.g., grantees, parents, Federal employees, contractors), specify the purpose for each type of individual.

EDSTAR collects and maintains PII to facilitate background investigation adjudications, confirm security clearance information, and manage physical access to Department facilities.

1.5. Is the IT system operated by the agency or by a contractor?

Agency

1.6. If the IT system is operated by a contractor, describe the contractor's role in operating the system.

☑ N/A

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

Click here to select.

☑ N/A

2. Legal Authorities and Other Requirements

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

2.1. What specific legal authorities permit and regulate the collection and use of data by the IT system? Include name and citation of each authority.

The authorities for collecting, maintaining, and using information for the purposes identified above:

[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

- Homeland Security Presidential Directive (HSPD)-12: Policy for a Common Identification Standard for Federal Employees and Contractors
- 5 CFR 731: Suitability
- 5 CFR 732: National Security Positions
- 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

System of Records Notice (SORN)

2.2. Has the Department's Privacy Program determined that the PII maintained by the IT system is or will be maintained as part of a Privacy Act system of records? Refer to the "SORN" item in the "Privacy Program Determination" section of the PTA if unsure.

☒ Yes

☐ No

2.3. If yes, provide the full name(s), number(s), and Federal Register citation of the applicable SORN(s) and/or a statement indicating that a new or modified SORN is being prepared.

The SORN, "Investigatory Material Compiled for Personnel Security and Suitability, Positive Identification Verification and Access Control for the Department of Education Security Tracking and Reporting System (EDSTAR)" (18-05-17), was published in the Federal Register on November 27, 2007, at 72 FR 66158.

Records Management

If you do not know your records schedule, consult with your records liaison, or send an email to RMHelp@ed.gov

2.4. Is there an applicable records retention schedule(s) for the information maintained in the IT system? Note: If no records schedule is in place or you are unsure of the applicable records schedule, reach out to your records liaison or the Records Management Office.

☒ Yes, there is/are approved records retention schedule(s) for the information. List the schedule(s):

Disposition Authority Number: DAA-GRS-2021-0001-0007, Records of people not issued clearances.

- Destroy 1 year after consideration of the candidate ends, but longer retention is authorized if required for business use.

Disposition Authority Number: DAA-GRS-2021-0001-0008, Records of people issued clearances.

- Destroy 5 years after employee or contractor relationship ends, but longer retention is authorized if required for business use.

☐ No, there are currently no approved records retention schedules, but there is a proposed schedule or plan to establish a schedule. Explain:

2.5. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule ?

☒ Yes
☐ No

3. Information Collection, Maintenance, Use, and/or Disclosure

Collection

3.1. Select the types of PII that are collected, maintained, used, and/or disclosed by the IT system. **Note:** PII includes any information that is linked or linkable to an individual, including business or contact information, information that is publicly accessible elsewhere, and ordinarily non-sensitive information.

Biographical and Contact Information

☒ Name	☒ Date of Birth	☒ Gender or Sex
☒ City, State, or County of Birth	☒ Country of Birth	☒ Home Address
☒ Personal Phone Number	☒ Work Phone Number	☒ Personal Email Address
☒ Work Email Address	☒ Work Address	☐ Personal Fax Number

☐ Work Fax Number	☒ Digital Signature ☒ Hand Signature	☒ Mother's Maiden Name

Other Demographic Information

☒ Citizenship and/or Alien Registration Number (A-Number)	☒ Military Service	☒ Marital Status, Spouse, and/or Child Information (Specify below)
☒ Educational Background/Records	☐ Group/ Organization Membership	☒ Employment Information
☒ Physical Characteristics or Biometrics (Height, Weight, etc.)	☒ Race/Ethnicity	☐ Religion

Identification Numbers

☒ Social Security Number	☐ Truncated/Partial Social Security Number	☒ Driver's License Number
☒ Passport Number	☒ Employee Identification Number	☐ Professional License Number
☐ Credit/Debit Card Number	☐ Bank/Financial Account Number	☐ Personal Device Identifiers/Serial Numbers
☐ License Plate Number	☒ File/Case ID Number	☐ Federal Student Aid Number
☐ Student ID Number	☐ Student Loan Number	☐ Grant Number
☐ Other ID That Can Be Traced to Individual (Specify below)		

Electronic and Miscellaneous Information

☐ Username/User ID	☐ Password	☐ IP Address
☐ MAC Address	☐ Complaint Information (Specify below)	☐ Medical Information (Specify below)
☐ Location Data	☐ Log Data That Can Be Traced to Individual	☒ Photographs of Individuals
☐ Videos of Individuals	☒ Criminal history	☐ Other (Specify below)

If you have been directed to "specify below," describe the PII:

3.2. Select the category of individuals from whom information is collected, maintained, used, or disclosed by the IT system and, if applicable, list what information from Question 3.1 is collected from each. Check all that apply:

☒ Federal Employees

Specify types of information collected from Federal employees:

Maintained in Security Manager:

- Name
- Former names
- Birth date
- Place of birth
- SSN
- Home address
- Phone numbers
- Driver's license number
- Passport number
- Employment history
- Residential history
- Education history and degrees earned
- Citizenship
- 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
- Investigator notes
- Tax return information
- Credit reports
- Security violations, circumstances of violations, and agency actions taken

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

- Documentation related to arrests and convictions for violations of the law
- Reporting on interviews held with the individual, his or her present and former supervisors, co-workers, associates, neighbors, educators, and other associates
- Correspondence involving the individual related to adjudication of suitability investigations
- Reports of inquiries made of law enforcement agencies for information about the individual contained in the agencies' records

Maintained in WEBS:

- Fingerprints
- Name
- Height
- Weight
- Date of birth
- SSN
- Place of birth
- Country of citizenship
- Gender
- Race
- Eye color
- Hair color

Maintained in MyID (legacy information):

- Name
- Photo
- Fingerprints

- Date of birth
- Height
- Weight
- Hair color
- Eye color
- Gender
- Forms of identification (e.g., driver's license number, passport number)

☒ Federal Contractors

Specify types of information collected from Federal contractors:
The types of information collected for contractors are the same as Federal Employees. See above.

☒ General Public (Any individual not employed by the Department).

Specify categories of the general public (e.g., teachers, students, parents, institution representatives, grantees, State and local government employees), and the types of information collected from each:[2]

- Names, birth dates, addresses, and citizenship of relatives of Department employees and contractors undergoing background investigations
- Name, email address, and phone number of references provided by Department employees and contractors undergoing background investigations
- Witness statements
- Reporting on interviews held with the individual, his or her present and former supervisors, co-workers, associates, neighbors, educators, and other associates

3.3. What are the sources of PII collected, maintained, used, or disclosed by the IT system (e.g., individual, school, another agency, commercial sources)?

- Information pertaining to background investigations is electronically transmitted from DCSA systems to Security Manager.
- EDSTAR also receives Federal employee information including name, position, and position security level from the Federal Personnel Payroll System (FPPS) on a daily

[2] For example:
From students: name, email address, phone number.
From institution representatives: name, email address, username, password.

basis. This information is used by the Security Manager component of EDSTAR to determine if an employee is still in active status with the Department.

- As part of background investigations, individuals may submit additional information requested by Department OFO, Federal Student Aid (FSA), and Institute of Education Sciences (IES) personnel security teams.
- Information (two forms of identification) pertaining to PIV card issuance and Fair Credit Reporting Act information was received directly from individuals when the MyID component of EDSTAR was active. This information is currently only maintained as legacy information.
- Fingerprinting and associated information in WEBS is acquired directly from individuals.

3.4. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, webpage, database)?

For the background investigation process, information from DCSA is imported electronically into EDSTAR from two DCSA systems: eDelivery and PIPS. Information collected directly from individuals by personnel security teams and/or WEBS is collected through a paper or electronic form. Fair Credit Reporting Act information is collected from individuals through the Fair Credit Reporting Act form.

3.5. Privacy law and policy generally requires agencies to collect or maintain only the minimum amount of PII necessary to accomplish an authorized purpose. For each of the PII elements that are indicated in Question 3.1, please describe why the information is necessary.

The PII elements pertaining to background investigations in Security Manager are determined by DCSA, who manages the forms used for initial collection of this information. This PII is necessary for Department personnel security teams to determine suitability and fitness for employment within or contracted to the Department.

The PII elements collected via WEBS are required by DOJ and DCSA to conduct background and/or criminal history checks.

PII elements collected for MyID were previously required to verify an individual's identity for PIV card creation and issuance. These elements are maintained pursuant to an approved records retention schedule.

3.6. Who can access the information maintained in the IT system?

☒ Federal Employees

☒ Federal Contractors

☐ General Public (Any individual not employed by the Department)

3.7. How is the PII validated or confirmed to ensure the integrity or quality of the information (e.g., form restricting, verifying newly collected information matches previously collected information, account verification, periodically requesting system users verify their own information in the system)?

Initial validation of PII collected through the background investigation process is the responsibility of DCSA.

The Department receives potential alerts (e.g., arrests, violations) from the Office of Director of National Intelligence (ODNI) for ongoing evaluation for national security positions. Validation occurs by comparing alert data against employee information received from FPPS.

Information Use for Testing

3.8. Is the PII maintained in the IT system used for internal testing, training, and researching new applications or information systems?

No

3.8.1. If the above answer to question 3.9 is **YES**, are you authorized to use PII when such information is used for internal testing, training, and research?

☑ N/A

Click here to select.

3.8.2. If the above answer to question 3.9 is **YES,** what controls are in place to minimize the privacy risk and protect the data?

☑ N/A

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.

3.9. Does the IT system collect or maintain Social Security numbers (SSNs)?

Yes

3.9.1. If the above answer to question 3.10 is **YES**, cite the authority for collecting or maintaining the SSNs.

☐ N/A

The collection of SSNs that are maintained in this system is authorized by 5 U.S.C. 301 and Executive Order 9397, as amended by Executive Order 13478 (November 18, 2008).

3.9.2. If the above answer to question 3.9 is **YES**, explain the purpose for the collection/maintenance and how the SSNs are used.

☐ N/A

The system collects and maintains SSNs on all individuals whose information is maintained in the system. SSNs are obtained as a way of verifying the identity of individuals during investigations.

The SSN is disclosed internally within the Department for investigative purposes and is shared with other Federal agencies. The SSN is used to determine what clearances/investigations exist for individuals and other relevant information available from other Federal agencies.

3.9.3. If the above answer to question 3.9 is **YES**, specify whether the collection of the SSNs is mandatory or voluntary. What are the consequences for the individual of not providing the SSN, if any?

☐ N/A

EDSTAR processes individuals for security approval to work within the Department 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.

3.9.4. If the above answer to question 3.9 is **YES**, specify any alternatives to SSNs that were considered and explain why they were not used.

☐ N/A

SSNs are required for the purposes of the investigations as they are the only reliable method of matching individuals' information with existing records. Alternatives were considered, but the SSN is needed as part of the background investigation process as it is the standard identifier used across multiple entities.

4. Notice

4.1. How does the IT system provide individuals with a privacy notice about the collection, maintenance, use, and disclosure of PII prior to its collection? For example, does the IT system provide a Privacy Act Statement (if applicable) or other privacy notices provided at the point of collection? If a notice is not provided, explain why not.

For the background investigation process, notice is provided on forms submitted by prospective Federal employees and contractors. These forms are managed and initially received by DCSA.

For the credentialing process, a Privacy Act statement is provided on the Department's "Request for Personal Identification Verification" form (please see question 4.2).

Public notice is also provided by the publication of a SORN and this PIA.

4.2. If you, or a partner, maintain a program website that is not hosted on the ed.gov domain and is accessible to the public, does the program website have a webpage privacy policy?

☒ N/A

4.3. Provide a link to the webpage where the privacy notice referenced in Question 4.1 is posted. If there is no publicly accessible link, provide the text of the privacy notice. Do not include security banners, security notices, Paperwork Reduction Act statements, or other notices not specifically related to privacy.

☐ N/A

PRIVACY ACT STATEMENT: 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.

Failure to provide all of the requested information may result in ED being unable to process your request for a Personal Identity Verification Card (PIV), or denial of issuance of a PIV. If you do not have a PIV, you may not be granted access to ED facilities or networks, which could have an adverse impact on your application to become, or status as, an ED employee, contractor or affiliate where such access is required to perform your assigned duties or responsibilities.

4.4. What opportunities are available for individuals to consent to uses of their PII, decline to provide PII, or opt out of the project? If these options are not available, state why not.

EDSTAR processes individuals for security approval to work within the Department 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.

4.5. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practices, policies, or activities that affect the PII and the privacy risks to ensure that individuals are aware of and, where feasible, can consent to, these changes?

Yes

5. Information Sharing and Disclosures

Internal

5.1. Is PII maintained in the IT system shared internally with any other Department IT system(s) and/or principal offices? If the answer is **NO**, skip to Question 5.4.

Yes

5.2. Which categories of PII from Question 3.1 are shared and with which Department IT system(s) and/or principal offices?

☐ N/A

Contracting office representatives (CORs) and information system security officers (ISSOs) from other principal offices will have access to EDSTAR's Security Manager to verify investigation information and/or clearance level for system access requests. PII accessed will include identifiers such as name, date of birth, SSN, position, and background investigation status.

5.3. What is the purpose for sharing the specified PII with each Department IT system(s) and/or principal office specified in Question 5.2?

☐ N/A

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

External

5.4. Is PII maintained in the IT system shared with any external entities (e.g., another agency, grantee, school district, the public)? If the answer is **NO**, skip to Question 6.1.

Yes

5.5. Which categories of PII from Question 3.1 are shared and with whom?

☐ N/A

Individuals' fingerprints, height, weight, date of birth, name, SSN, place of birth, country of citizenship, gender, race, eye color, and hair color are shared with DCSA for the background investigation process and DOJ for criminal history checks. If a match is

made on a specific record, the information on the violation is provided to the Department.

5.6. What is the purpose for sharing the PII with each external entity specified in Question 5.5?

☐ N/A

PII is shared with DCSA and DOJ to initiate and validate background investigations.

5.7. What are the specific authorities that authorize sharing the PII with the external entities specified in Question 5.5?

☐ N/A

5 CFR 731: Suitability and Executive Order 9397.

5.8. Does the IT system maintain an accounting of any disclosures made to an external entity?

☐ N/A

Yes

5.8.1. If so, is the accounting of disclosures made to external entities available in response to a Privacy Act request?

Yes

5.9. How is the PII shared with the external entity (e.g., encrypted email, transport layer security (TLS) line)? Specify whether the PII is encrypted in transit and state the encryption method that is used.

☐ N/A

PII is shared via connections with DOJ and two DCSA systems: eDelivery and PIPS. The information is shared with both agencies using encrypted virtual private network tunnels.

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

☐ N/A

Yes

5.11 Does the project allow for the PII to be redisclosed by the external entities or require the external entities to request permission prior to its redisclosure? If so, describe the limitations on redisclosure and how they are documented and enforced.

☐ N/A

No

6. Redress

6.1. What are the procedures that allow individuals to access their own information in the IT system? If there are no such procedures, state why not.

The Secretary has exempted by regulation (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.

Although EDSTAR is exempt, an individual may nonetheless request notification of or access to a record in the system.

If an individual wishes to determine whether a record exists, or wishes to access a record, 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, SSN, 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.

6.2. What procedures are in place to allow individuals to correct or amend inaccurate or erroneous information?

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 response provided in question 6.1, 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.

6.3. How does the program or IT system notify individuals about the procedures for accessing or correcting their information?

Individuals are notified of this system's exemption and procedures for correcting information 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 ISSO to build privacy and security safeguards into the IT system?

Yes

7.2. Is an authorization to operate (ATO) required for the IT system?

Yes

7.2.1. If the answer to Question 7.2 is **YES**, does the IT system have an active ATO?

Yes

7.3. What is the NIST Federal Information Processing Standard 199 security categorization of this IT system?

☐ Low

☒ Moderate

☐ High

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

EDSTAR is maintained on secure computer servers located in one or more secure network server facilities. 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 which users must acknowledge and sign prior to receiving access to the system.

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), EDSTAR must receive a signed ATO from a designated FSA official. FISMA controls implemented by EDSTAR are comprised of a combination of management, operational, and technical controls. All users have a specific role assigned to them approved by the Information System Security Officer (ISSO) and are required to utilize a complex password and two-factor authentication.

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

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

8. Auditing and Accountability

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

The system owner ensures that the information is maintained and used in accordance with the stated practices in this PIA.

The first method is by completing the Department's risk management framework process to receive an ATO. During the ATO process, the EDSTAR system owner

ensures that National Institute of Standards and Technology (NIST) Special Publication 800-53 controls are implemented. The NIST controls include administrative, technical, and physical controls to ensure that information is used in accordance with approved policies and practices.

The system owner ensures the information is used in accordance with stated practices by confirming that the privacy risks are properly assessed, and the data are secured, ensuring appropriate security and privacy controls are implemented to restrict access, and to properly manage and safeguard PII maintained within the system. The system owner participates in all major security and privacy risk briefings, meets regularly with the ISSO to addresses security and privacy risks throughout the system's lifecycle. Additionally, the system owner regularly reviews signed agreements that govern data use between organizations, such Memorandums of Understanding (MOUs), and other information sharing agreements.

8.2. How does the ISO continuously monitor and audit the security and privacy controls to ensure effective implementation and safeguarding of PII?

Continuous Diagnostics and Mitigation (CDM) scans are produced on a weekly basis to identify security and privacy vulnerabilities which are reviewed by the system owner and ISSO. In the review, system owners are notified of any findings that require action. EDSTAR also participates in the Ongoing Security Authorization (OSA) program and continuous monitoring program, which provide quarterly reviews of FISMA controls and continuous scans to ensure that security and privacy controls are in place and working properly. EDSTAR has a regular patching cycle to ensure the system is secured with the most up-to-date capabilities.

The system owner, in coordination with the ISSO and Security Assessment Team (SAT), ensures the information is used in accordance with stated practices by confirming that the privacy risks are properly assessed and that all data are secured, ensuring appropriate security and privacy controls are implemented to restrict access, and properly managing and safeguarding PII maintained within the system. EDSTAR will also participate in annual assessments and audits as required, to ensure the effective safeguarding of PII.

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

Privacy risks associated with EDSTAR include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII are potentially hazardous to both individuals and organizations. Individual harm may include identity theft,

embarrassment, or financial loss. Organizational harm may include a loss of public trust, legal liability, or remediation costs.

The risks are mitigated by the above-mentioned safeguards, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department. To further mitigate this risk, the following safeguards have been implemented:

- Monthly vulnerability scans
- Annual contingency plan test
- Annual or ongoing security assessments

Risks are also mitigated by updating security patches per the patch scheduling and updating devices operating software, amongst other software. System patching is performed monthly, and scans are run on the production environment each month in support of the monthly patching cycle. Collecting the minimum PII necessary to achieve the system's purpose also mitigates privacy risks.