Privacy Impact Assessment (PIA)

for the

Education Security Tracking and Reporting System (EDSTAR)

May 11, 2022

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: Kimberley Dean/EDSTAR Program Manager
Contact Email: Kim.Dean@ed.gov

System Owner

Name/Title: D'Mekka Thompson/Information System Owner
Principal Office: Office of Finance and Operations

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

*Please complete this **Privacy Impact Assessment (PIA)** on 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, please answer with N/A.

1. Introduction

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

The U.S. Department of Education (Department) Security Tracking and Reporting System (EDSTAR) is a background investigation, security clearance, Personal Identity Verification (PIV) ID issuance and physical access control, and 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, issue Homeland Security Presidential Directive-12 (HSPD-12) compliant PIV IDs, control physical access, and monitor security mechanisms for all Department employees and contractors.

The implementation and deployment of EDSTAR is driven by the HSPD-12 directive, which requires a 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.

Employees and contractors are provided with PIV IDs through a process of enrollment. This occurs at enrollment stations, some of which are portable and able to be moved to locations outside of Department headquarters to enroll Federal employees and contractors. The enrollment stations collect applicant data and then send these data to various EDSTAR components via the Department's virtual private network (VPN). The enrollment stations are composed of desktop and laptop computers, a fingerprint capture and reader device, a scanner, and a digital camera.

EDSTAR applications for background investigations and PIV issuance include:

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 other applications outside of EDSTAR such as 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. Once this information is transferred to Security Manager, Department personnel with appropriate background investigation and roles can view the updated case files and make adjudicative decisions on background investigations. Security Manager also interfaces with enrollment stations and MyID to create an automated PIV card issuance system.

WEBS (CrossMatch): WEBS collects employee/contractor fingerprint and personal data. WEBS sends data to the Security Manager system using an XML interface that matches the data in the Security Manager file for current Federal employees and contractors. For onboarding employees and contractors, WEBS interfaces with the U.S. Department of Justice (DOJ) Civilian Applicant System (CAS) or the Defense Counterintelligence and Security Agency (DCSA), for criminal history record checks.

MyID (Intercede): MyID is a card management system that stores employee/contractor credential information. Each PIV card will contain a certificate which allows the user to be authenticated on the network, digitally sign documents, and encrypt and securely send email messages. MyID houses those certificates and, in the event that those certificates need to be recovered for any reason (damage, system goes down, etc.), MyID keeps them in escrow (storage) so they can be easily recovered and reissued. The MyID receives validated case information from the enrollment system (WEBS) and the Security Manager System to validate that the individual is eligible for issuance of a PIV card.

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 the closed circuit TV cameras, monitors, and access control. The ID Access control portion of DSX communicates with card readers via XML to receive cardholder ID information.

1.2. Describe the purpose for which the personally identifiable information (PII)[1] is collected, used, maintained or shared.

[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

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

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

This PIA is being updated as part of a regular biennial review.

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.

The authorities for collecting, maintaining, and using information for the purposes identified in question 1.2 are:

- Homeland Security Presidential Directive (HSPD)-12.
- 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

This information is retrieved by searching one or more of the following fields: Unique Identifier (Person Handle),[2] Social Security number (SSN), and name.

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)).[3] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

☐ N/A

The System of Records Notice, "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)", SORN Number: 18-05-17 was published to the Federal Register on November 27, 2007.

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

[2] Unique number assigned to each individual undergoing security clearance investigation that is tracked through Security Manager.

[3] 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

Records Management
If you do not know your records schedule, please consult with your records liaison or send an email to 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.

2.4. 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.

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. The system includes:

- Name
- Former names
- Birth date
- Birthplace
- SSN
- Fingerprints
- Home address
- Phone numbers

- Employment history
- Residential history
- Education and degrees earned
- Names and contact information of associates and references
- Citizenship
- Names, birth dates, and addresses 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 violations, and agency actions taken

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

- Documentation as 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

For more detail on information collected through background investigations, please reference the Electronic Questionnaire for Investigations Processing (eQIP) PIA.

In addition to the information listed above, EDSTAR may also obtain information related to a particular background investigation during the course of the investigation.

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

Yes

The PII collected and maintained is the minimum amount required by EDSTAR. EDSTAR collects and maintains PII to facilitate background investigation adjudications, track security clearance information, issue PIV cards, and manage physical access to Department facilities. Information collected is needed to ensure the individual seeking a security clearance or access to Department facilities or systems are fully vetted and cleared.

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

- Information pertaining to background investigations is acquired from the DCSA, the entity responsible for the initial collection of this information.
- EDSTAR also receives Federal employee information including name, position, and position security level from the Federal Personnel Payroll System (FPPS) on a daily basis. This information is used by the Security Manager component of EDSTAR for the purposes of understanding if an employee is still in active status with the Department.
- As part of the investigation, individuals may submit information requested by Personnel Security.
- Information (two forms of identification) pertaining to PIV card issuance, Fair Credit Reporting Act information, and fingerprinting is received directly from individuals.

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

For the background investigation process, information from DCSA is imported electronically into EDSTAR from two DCSA systems: eDelivery and the PIPS. Information collected directly from individuals by Personnel Security is collected through

a paper or electronic form.[4] Fair Credit Reporting Act information is collected from the individual by the Department through the Fair Credit Reporting Act form.

For the PIV issuance process, information is collected from the individual by the Department through forms. Information is collected through the following:

- Request for Personal Identification Verification, February 2016
- Two forms of identification are collected/scanned as part of the PIV issuance process
- Fingerprints (Fingerprint card FD-258)
- DoJ system, CAS

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[5] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

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 Personnel Security Office may further validate the data.

Throughout the individual's background investigation process, the Personnel 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.

Ongoing evaluation for national security positions are based on potential alerts that are received by the Department (e.g., arrest, violations). Validation occurs by comparing employee data against the information received from FPPS.

Use

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

This information is used to verify individuals' background information, make adjudication determinations concerning suitability for Federal employment and suitability for contract positions, manage access to the Department's facilities and information systems, including restricted areas, and facilitate the issuance of PIV cards.

[4] DCSA 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.

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

No

3.7.1. If the above answer is **YES,** what controls are in place to minimize the 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.

3.8. 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 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 listed in Question 5.5. The SSN is used to determine what clearances/investigations exist on individuals or other relevant information available from other Federal agencies. The SSN is disclosed and exchanged with State/local governments to gather investigative data and records through secure tunnels and can only be accessed by authorized personnel.

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

☐ N/A

SSNs are required for the purposes of the investigations as they are the most reliable method of matching individuals' information with existing records. Since the SSN is a unique identifier, it presents the best method to ensure information collected about an individual pertains to the individual. The SSN is disclosed and exchanged with State/local governments to gather investigative data and records through secure tunnels and can only be accessed by authorized personnel. 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 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.

For the background investigation process, most of the information is collected through the e-Qip process, and notice provided on those forms.

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).

In addition, the system provides public notice by publishing 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

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.

4.3. 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 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

Contracting office representatives (CORs) and information system security officers (ISSOs) from other principal offices will have access to EDSTAR's Security Manager to verify information such as investigation or clearance level for system/facility 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 the specified internal organizations?

☐ 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. 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.[6]
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, SSN, home address, and phone numbers are shared with DCSA for the background investigation process and fingerprints are submitted to DOJ for criminal 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 the specified external entities?

☐ N/A

[6] 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.

PII is shared with DCSA and DOJ to initiate and continuously validate 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: eDelivery and PIPS. The information is shared with both agencies using encrypted virtual private network tunnels.

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

No

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 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, 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.

6.2. What procedures are in place to allow the subject individual to correct 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 project notify individuals about the procedures for 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 CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

Yes

7.2. Is an Authorization to Operate (ATO) required?

Yes

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?

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 (ROB) 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) and Office of Management and Budget (OMB) policy, EDSTAR must receive a signed ATO from a designated Department authorizing official. Security and privacy controls implemented by EDSTAR are comprised of a combination of administrative, physical, and technical controls.

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.

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?

Yes

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.

The following tasks are performed to safeguard EDSTAR information:

- Monthly vulnerability scans performed
- Annual contingency plan test performed
- Annual self-assessments conducted; and/or annual security assessments performed by the Department Security Authorization Team
- Annual updates to system security documents
- Annual mandatory Cybersecurity and Privacy Training for employees and contractors
- Monthly Continuous Monitoring is in place with vulnerability scans (RA- 05), hardware/software inventories (CM-08), and configuration management updates (CM-06) are posted to the Department's tracking system

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. The system owner also works directly with the privacy program 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 National Institute of Standards and Technology (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?

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.