Privacy Impact Assessment (PIA)

for the

Information Assurance Services Tools

April 23, 2024

Point of Contact

Contact Person: Miguel Calin
Title: Information System Owner
Email: Miguel.Calin@ed.gov

System Owner

Name: Miguel Calin
Title: Information System Owner
Principal Office: OCIO

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 Information Assurance Services Tools (IAST) system serves as a U.S. Department of Education (Department) central repository for applications and subsystems used and managed by the Security Engineering and Architecture (SE&A) Branch of the Information Assurance Systems Division of the Office of the Chief Information Officer (OCIO).

The current set of applications that falls under IAST includes DB Protect, Department Continuous Diagnostics and Mitigation (CDM), EnCase Endpoint Investigator (EnCase), Information Security Continuous Monitoring (ISCM), Mission Intelligence Visualization Services (MIVS) Power BI Gateway (MIVS PBIG), Penetration Testing Laptop, RedSeal, Tenable, and WebInspect. These components are standalone applications or tools but are being authorized under one system boundary.

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

Components of IAST are standalone tools that include software, hardware, or a combination of both. User authentication for access to the components of IAST is conducted through the Department's Identity, Credential, and Access Management (ICAM) system. An overview of each component's function is provided in the table below:

Tool	Function
DB Protect	DB Protect is a data security platform that uncovers database configuration mistakes, access control issues, missing patches, or any combination of settings that could lead to the escalation of privileged attacks, data leakage, denial-of-service (DoS) attacks, or unauthorized

Tool	Function
	modification of data held within data stores (e.g., relational databases and Big Data). All Department databases other than those within Federal Student Aid (FSA) (which have their own vulnerability detection software) are subject to DB Protect scans.
CDM-ED	CDM-ED is an application that monitors hardware and software across the Department's network for vulnerabilities and compliance with security technical implementation guides. CDM-ED is the Department's implementation of a dashboard maintained by the Department of Homeland Security (DHS) that aggregates and transforms data collected from Department network sensors. The dashboard uses the data to calculate risk scores for vulnerabilities or compliance failures based on severity, the length of time the vulnerability has been on the network, and if the device seen on the network is documented in a system boundary's authoritative hardware inventory record. Data is refreshed and sent to the dashboard daily. Examples of data collected: hostname, IP address, MAC address, device serial number, date the device was last seen, email addresses of the Information System Owner (ISO) and the Information System Security Officer (ISSO) responsible for the devices, and system boundary details such as its CIA rating and authorization and expiration dates.
EnCase Endpoint Investigator	EnCase is software used for forensic, cybersecurity, and security analytics. Encase is used to recover evidence from hard drives in investigations of cybersecurity events and incidents. EnCase allows the investigator to conduct an in-depth analysis of user files to collect evidence such as documents, pictures, internet history, and Windows Registry information. The collection of PII by EnCase is incidental and unintentional. For example, if an endpoint that is the subject of an investigation has stored PII in a hard drive or document, EnCase collects that stored PII when it collects the image of that hard drive or the document. An endpoint is a remote computing device that communicates with a network to which it is connected. Examples of endpoints are laptops, desktops, and smartphones.
Information Security Continuous Monitoring	ISCM servers use software development tools to help automate the generation of comprehensive hardware inventories of various system boundaries from CSAM. This automation ensures continuous monitoring capabilities have a current list of all hardware assets and their FISMA boundaries. This information is currently being used to support the Cyber Infrastructure and Security Agency's (CISA) Binding Operational Directive (BOD) 23-01 and the CDM program reporting requirements. The data also feed into dashboards within the Department Cyber Data Lake (EDCDL) which report system behavior and risk to system owners.
MIVS Power BI Gateway Server	The MIVS Power BI Gateway Server is a Windows server that hosts the Microsoft On-Premises Data Gateway, a software application that provides quick and secure data transfer between on-premises systems

Tool	Function
	(such as CSAM, Splunk, and ServiceNow) and Microsoft cloud services (such as Power BI). Data facilitated through the data gateway are primarily used for the Cybersecurity Framework (CSF) Scorecard, which supports risk analysis for Department systems by providing scores that rate systems' compliance with various requirements. Data transferred through the data gateway includes plans of action and milestones (POA&Ms), asset information, asset vulnerabilities, and system security artifact information.
Penetration Testing Laptop	The Penetration Testing Laptop is a laptop that is built on the Windows Golden Image and maintained the same way as other laptops on the Department network. This laptop also hosts virtual machines that are running Windows and Linux operating systems not supported by the Department and are loaded with software intended to test the effectiveness of security controls during a penetration test. These tests include attacks on application APIs, attempts to subvert firewalls, and potentially deploying malicious scripts or software that will allow the penetration tester to launch an attack or open communications for the penetration tester. The end goal is to document and report the effective security controls and bring attention to any security controls that need improvement.
RedSeal	RedSeal is an application that creates analytic platforms for businesses and government agencies to visualize their security architecture, continuously audit, monitor IT compliance, and eliminate cyber threats. RedSeal performs an analysis of network connectivity and endpoint vulnerabilities, adds configuration files from switches, routers, firewalls, and load balancers, and imports host and vulnerability data from vulnerability scanners and other sources.
Tenable	Tenable Security Center (Tenable) is a management application for vulnerability scanning of all non-FSA endpoints within the Department. Tenable's dashboard provides an overview of scan results, intrusion detection, and monitoring of valuable network assets. Tenable scans all endpoints and identifies endpoints that contain vulnerabilities as identified by Tenable plugins.
WebInspect	WebInspect is a tool designed to detect security flaws in web-based applications. This session-based assessment reports each vulnerability, pinpoints locations in the application, and recommends corrective actions. All non-FSA Department systems that have web servers or web application interfaces are subjected to WebInspect scans.

IAST users include SE&A system administrators (i.e., OCIO Vulnerability Management Program Enhancements Team, OCIO Vulnerability Management Team, and the Department Security Operations Center (EDSOC)) as well as any other users approved by the IAST system owner. Access to IAST components is controlled through role-based access.

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.

EnCase and Penetration Testing Laptop may incidentally encounter and collect PII. EnCase is an application used for forensic, cyber security, and security analytics that recovers evidence from hard drives in investigations of cybersecurity events and incidents. If an endpoint that is the subject of an investigation has stored PII in a hard drive or document, EnCase collects that stored PII when it collects the image of that hard drive or the document. The Penetration Testing Laptop is loaded with software intended to test the effectiveness of security controls during a penetration test and could encounter PII during a testing exercise.

CDM-ED is an application that monitors hardware and software across the Department's network for vulnerabilities and compliance with security technical implementation guides. Email addresses of ISOs and ISSOs responsible for devices on the Department's network are collected by CDM to establish areas of responsibility and track compliance with security technical implementation guides.

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

Agency

[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

1.6. 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 the name and citation of each authority.

44 U.S.C. § 3553. Authority and functions of the Director and the Secretary, Part (a), Subpart (2) requires agencies: "to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of —
(A) Information collected or maintained by or on behalf of an agency; or
(B) Information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency".

44 U.S.C. § 3554. Federal agency responsibilities, Part (a), Subpart (7) requires: "(b) AGENCY PROGRAM. — Each agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

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.

N/A

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):

- GRS 3.2, item 010: Systems and data security records.
  - TEMPORARY. Destroy 1 year(s) after the system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system.
- GRS 3.2, item 020: Computer security incident handling, reporting, and follow-up records.
  - TEMPORARY. Destroy 3 years after all necessary follow-up actions have been completed, but longer retention is authorized if required for business use.
- GRS 3.2, item 031: System access records; Systems requiring special accountability for access.
  - TEMPORARY. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.
- GRS 3.2, item 035: Cybersecurity logging records; Full packet capture data.
  - TEMPORARY. Destroy when 72 hours old. Longer retention is authorized for business use.

- GRS 3.2, item 036: Cybersecurity logging records; Cybersecurity event logs.
    - TEMPORARY. Destroy when 30 months old. Longer retention is authorized 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:

Any data that resides within a Department system or device may be collected by EnCase during an investigation or by the Penetration Testing Laptop during a penetration test.

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:

Any data that resides within a Department system or device may be collected by EnCase during an investigation or by the Penetration Testing Laptop during a penetration test.

Email addresses of ISOs and ISSOs are collected by CDM.

☒ Federal Contractors

Specify types of information collected from Federal contractors:

Any data that resides within a Department system or device may be collected by EnCase during an investigation or by the Penetration Testing Laptop during a penetration test.

Email addresses of ISOs and ISSOs are collected by CDM.

☒ 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]

Any data that resides within a Department system or device may be collected by EnCase during an investigation or by the Penetration Testing Laptop during a penetration test.

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)?

Work email addresses of Federal employees and contractors are collected from CSAM and EDServiceNow.

Data collected by EnCase and the Penetration Testing Laptop are acquired from devices, systems, or documents subject to investigation and/or testing.

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

PII is encountered and collected by EnCase and the Penetration Testing Laptop during the investigation and/or testing of Department devices, systems, or documents.

Department ISO and ISSO work email addresses are transmitted to CDM from CSAM via a direct connection.

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.

For EnCase and the Penetration Testing Laptop, specific elements of PII are not solicited. PII may be incidentally collected during investigations of cybersecurity events or incidents using EnCase and during penetration tests conducted using the Penetration Testing Laptop.

Email addresses of ISOs and ISSOs responsible for devices on the Department's network are collected by CDM to establish areas of responsibility and track compliance with

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

security technical implementation guides.

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)?

PII for EnCase and the Penetration Testing Laptop is collected incidentally as part of an investigation and/or penetration test, therefore it is not validated.

ISO and ISSO email addresses are validated at the source system level in EDServiceNow and CSAM.

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

44 U.S.C. § 3553. Authority and functions of the Director and the Secretary, Part (a), Subpart (2) requires agencies: "to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of

(A) Information collected or maintained by or on behalf of an agency; or
(B) Information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency".

44 U.S.C. § 3554. Federal agency responsibilities, Part (a), Subpart (7) requires: "(b) AGENCY PROGRAM. — Each agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

3.10.2. If the above answer to question 3.10 is YES, explain the purpose for the collection/maintenance and how the SSNs are used.

□ N/A

EnCase and the Penetration Testing Laptop are the only IAST components that could potentially collect and store SSNs. For example, when EnCase collects an image of a hard drive or document from a computer under investigation, EnCase encounters any PII, including SSNs, stored in the hard drive or document.

3.10.3. If the above answer to question 3.10 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

As stated in Question 3.10.2, IAST does not intentionally collect SSNs or other PII. Incidental collection of PII may be necessary as part of an investigation of hard drives or documents.

3.10.4. If the above answer to question 3.10 is YES, specify any alternatives to SSNs that were considered and explain why they were not used.

□ N/A

The system does not intentionally collect SSNs or other PII. For investigation purposes, an SSN could incidentally be collected but is not used as part of the security analysis.

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.

IAST does not collect PII directly from individuals, therefore notice is not provided. Notice for collection of ISO and ISSO email addresses is provided at the source system level.

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

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.

Since the collection of PII via EnCase and the Penetration Testing Laptop is incidental and information collected from Department employees and contractors is necessary for performing their job functions, there are no opportunities for individuals to opt out of the collection.

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?

N/A

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.

No

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

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

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.

No

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

☑ N/A

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

☑ N/A

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

☑ N/A

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

☑ N/A

Click here to select.

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

N/A

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

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

Click here to select.

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

Click here to select.

6. Redress

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

Users do not have access to their information in IAST. Users that wish to access or amend information originating in EDServiceNow or CSAM would do so in the source system. Individuals cannot access or amend information obtained through EnCase or the Penetration Testing Laptop as this information is obtained through investigations.

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

Users may not amend their information in IAST. Users that wish to access or amend information originating in EDServiceNow or CSAM would do so in the source system. Individuals cannot access or amend information obtained through EnCase or the Penetration Testing Laptop as this information is obtained through investigations.

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

Since individuals cannot access or correct their information in the system, IAST does not notify individuals of procedures for accessing or correcting their information.

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?

IAST component tools are hosted within a secure environment in the IBM Smart Cloud for Government (IBM SCG).

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

Access to the IAST components is restricted to authorized users who have authenticated to the Department's network using their Department-issued Personal Identity Verification (PIV) card. Access to all privileged roles is controlled through processes that enforce formal requests and approvals for access on a need-to-know and least-privilege basis. Strict separation of duties is also in place. Access to data is protected through physical access controls to hosting facilities, firewalls, network and host intrusion detection systems, event monitoring systems, nightly backups, and data encryption while at rest and in transit. Additionally, there are scheduled system audits, user recertifications, and vulnerability scans.

Only authorized EnCase and Penetration Testing Laptop users (i.e., investigators and penetration testers) may encounter PII while managing those components of IAST. All users of EnCase and the Penetration Testing Laptop are authenticated via Department-approved PIV cards.

IAST uses access control lists, firewalls, intrusion protection systems, FIPS-140 validated encryption, multifactor authentication, antimalware, and multiple cybersecurity capabilities to protect information.

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 IAST system owner ensures that the 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 and meets regularly with the ISSO. Additionally, the system owner regularly reviews signed agreements that govern data use between organizations such as 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?

IAST participates in the Ongoing Security Authorization (OSA) program and continuous monitoring program, which provides quarterly reviews of FISMA controls and continuous scans to ensure that security and privacy controls are in place and working properly. IAST has a regular patching cycle to ensure the system is secured with the most up-to-date capabilities.

The system owner ensures that IAST system administrators complete monthly reviews of audit logs to ensure there is no misuse or malicious activity with the system or data.

The system owner reviews audit reports provided by IAST administrators regarding information processing and maintains the access control list of who can access PII on a quarterly basis. The IAST system will also undergo annual OMB Circular A- 123, Appendix A (Management's Responsibility for Enterprise Risk Management and Internal Control) assessment, and NIST Special Publication 800-53 system security control self-assessments.

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 IAST include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII, and credentials 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, utilizing least privilege principles, masking SSNs, encrypting data in transmission, 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 regularly updating security patches and device operating 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.