Privacy Impact Assessment (PIA)
for the

Information Assurance Services Tools
December 8, 2021

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: Roman Kulbashny Branch Chief, Security Engineering and Architecture Branch
Contact Email: Roman.Kulbashny@ed.gov

System Owner

Name/Title: Roman Kulbashny Branch Chief, Security Engineering and Architecture Branch
Principal Office: Office of the Chief Information Officer

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 Information Assurance Services Tools (IAST) system serves as a U.S. Department of Education (Department) central repository for several tools and applications 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 EnCase Endpoint Investigator (EnCase), DB Protect, WebInspect, RedSeal, and Tenable. These applications are standalone applications or tools but are being authorized under one system boundary.

- EnCase is software used for forensic, cyber security, 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 in-depth analysis of user files to collect evidence such as documents, pictures, internet history, and Windows Registry information. EnCase is currently the only IAST component that collects PII; this collection is incidental and unintentional. For example, if an endpoint that is the subject of an investigation had 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.
- 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 escalation of privileged attacks, data leakage, denial-of-service (DoS), or unauthorized 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 subjected to DB Protect scans.
- 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.

- RedSeal is an application that creates analytic platforms for the Department to visualize their security architecture, continuously monitor information technology (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 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.

The primary users of IAST are SE&A Branch system administrators, including the OCIO Vulnerability Management Program Enhancements Team (VMPE), the OCIO Vulnerability Management Team (VM), and the Department Security Operations Center (EDSOC). Further users include Department users that would be approved by the Information System Owner. All access to the tools in IAST is controlled through role-based access.

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

EnCase is currently the only IAST component tool that has the possibility to encounter and incidentally collect PII. EnCase is software used for forensic, cyber security, and security analytics. Encase is used to recover evidence from hard drives in investigations of cybersecurity events and incidents. For example, if an endpoint that is the subject of an investigation had 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.

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

New System

[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

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

New PIA

Since this is a new system which could collect PII, a PIA is required.

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.

In accordance with the Federal Information Security Modernization Act (FISMA) of 2014 (Public Law 113–283), the Department has established an enterprise-wide Information Security Program (ISP) to safeguard the confidentiality, integrity, and availability of its information and systems. PII incidentally encountered and collected by IAST is initially collected in compliance with the Department's overarching Cybersecurity Policy OCIO-3-112, to analyze, identify, alert and prevent the unintentional or deliberate exfiltration of unprotected sensitive data from the Department's network. The Cybersecurity Policy is based on legislative, statutory, and executive directive requirements that include Federal laws and regulations, Presidential Directives and Executive Orders, Federal IT Acquisition Reform Act (FITARA), FISMA, the National Institute of Standards and Technology (NIST) Special Publications (SP) 800 series, the NIST Federal Information Processing Standards (FIPS), and Office of Management and Budget (OMB) memoranda. The Department has an obligation under Federal law to define and operate an effective cybersecurity program.

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?

No

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

☑ N/A

Click here to enter text.

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

The information is not retrieved by a personal identifier; the PII encountered and collected by IAST is incidental and never used in security analysis.

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.

General Records Schedule (GRS) 3.2, Item 010 Systems and data security records. Temporary. Destroy 1 year(s) after 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.
DAA-GRS2013-0006- 0001
General Records Schedule (GRS) 3.2, 020 Computer security incident handling, reporting and follow-up records

[2] A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. https://connected.ed.gov/om/Documents/SORN-Process.pdf

Temporary. Destroy 3 year(s) after all necessary follow-up actions have been completed, but longer retention is authorized if required for business use.
DAA-GRS2013-0006- 0002

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.

Any PII that is included in Department systems, such as Social Security number, (SSN), name, credit card number, email address, password, and username, could be encountered and incidentally collected by EnCase during an investigation.

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

Yes

EnCase is the only IAST component that encounters PII, and this is done incidentally and unintentionally. EnCase is software used for forensic, cyber security, and security analytics. Encase is used to recover evidence from hard drives in investigations of cybersecurity events and incidents, therefore may collect PII as part of the investigation. PII is encountered and collected incidentally by EnCase though electronic means. For example, when EnCase collects an image of a hard drive or document from a computer under investigation, EnCase encounters any PII stored in the hard drive or document. The information collected is the minimum amount to address the investigation.

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

Any member of the public that has information in Department systems that is collected by EnCase. Please refer to the PIAs for other Department systems to understand the sources of the PII in those systems.

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

PII is encountered and collected incidentally by EnCase though electronic means. For example, when EnCase collects an image of a hard drive or document from a computer under investigation, EnCase encounters any PII stored in the hard drive or document.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[3] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

Since the PII is collected incidentally and it is not used for security analysis purposes, it is not validated.

Use

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

PII is collected incidentally and not used for security analysis purposes.

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

Click here to enter text.

Social Security Numbers

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

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

[3] Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

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

EnCase is the only IAST component 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.

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

□ 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 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.

Since the collection of PII in IAS Tools is incidental and the PII is not used for security analysis, no notice is provided. Please refer to the PIAs for other Department systems to understand the notice that was provided prior to collection of the information.

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

Click here to enter text.

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?

Since collection of PII by IAST is incidental and unintentional, there are no opportunities for individuals to opt out of collection. Please refer to the PIAs for other Department systems to understand opt-out opportunities.

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?

N/A

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.

No

5.2. What PII will be shared and with whom?

☑ N/A

Click here to enter text.

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

☑ N/A

Click here to enter text.

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.

No

5.5. What PII will be shared and with whom? List programmatic disclosures only.[4] **Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose**.

☑ N/A

Click here to enter text.

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

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

☑ N/A

Click here to enter text.

5.7. Is the sharing with the external entities authorized?

☑ N/A

Click here to select.

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

☑ N/A

Click here to select.

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

☑ N/A

Click here to enter text.

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

Click here to select.

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

☑ N/A

Click here to select.

6. Redress

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

Individuals do not have access to their own information in IAST, as all PII collected through the system is incidental and unintentional. Please refer to the PIAs for other Department systems to understand the access procedures for those systems.

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

PII is incidentally and unintentionally collected as part of security event monitoring; individuals cannot correct any information collected by IAST. Please refer to the PIAs for other Department systems to understand the correction procedures for those systems.

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

PII is incidentally and unintentionally collected as part of security event monitoring; individuals cannot correct any information collected by IAST. Please refer to the PIAs for other Department systems to understand the correction procedures for those systems.

7. Safeguards

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

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

Yes

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

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?

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

Access to the IAST components is restricted only to users who have been authorized and 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. Enhancing this model, strict separation of duties is in place as well with regards to the distribution of roles. Access to data is protected through physical access controls to the 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 recertification, and vulnerability scans.

Only authorized EnCase users, specifically, the investigator assigned to a case, could encounter PII while managing the EnCase component of IAST. The system administrators do not have access to the PII. All users of EnCase are connected to EnCase via Department-approved PIV.

IAST uses access control lists (ACLs), firewalls, intrusion protection systems (IPS), FIPS-140 validated encryption, multi-factor authentication, antimalware, and multiple cybersecurity capabilities to protect the information. PII is encrypted at rest within the system boundaries of IAST. These security measures limit data access to Department and contract staff on a need to know basis and control individual users' ability to access information within the system.

Finally, all privileged users are provided a copy of the Rules of Behavior and are required to complete the annual Cybersecurity and Privacy Awareness training.

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.

IAST is reviewed annually and as needed when significant changes to the system occur. As part of the Department's continuous monitoring program, IAST is expected to review and renew the authorization to operate on a regular basis via the ongoing assessment and authorization process. This process includes audits of the implemented security and privacy controls by independent assessors. Findings from these audits produce Plans of

Actions and Milestones (POA&Ms) for the system owner to remediate. Self-assessments are also conducted on a continuous basis, including annual incident response and contingency plan testing. On a more frequent basis, vulnerability and compliance scans are performed to check for vulnerabilities and deviations from the Department standards.

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 ensures the IAST systems 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 the IAST administrators regarding information processing and maintains the access control list of who can access PII, on a quarterly basis. The system owner also works directly with the Department's privacy office on privacy compliance documentation to ensure all information in this PIA is up to date and accurate. Ultimately, the IAST system will 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.

Finally, the system owner documents the privacy controls every two years through the PIA review process. These privacy controls are then assessed by the security authorization team and the privacy office.

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?

Risks to privacy include unauthorized access, as well as mishandling and misuse of the information maintained in IAST.

To mitigate these privacy risks, IAST operates a comprehensive security program over the entire system and its supporting business processes. A key component of the security program is the continuous monitoring effort which ensures that the security and privacy controls remain effective over-time and that new threats are assessed, and appropriate countermeasures implemented.

The risk of unauthorized access to PII is mitigated through an array of safeguards, including strict access controls, segregation of duties, physical access controls at the hosting facility, data encryption (both in flight and at rest), annual access certifications, and network and host-based intrusion detection systems. All user access is approved via established Department Privilege User Access process. IAST access is authorized only from internal network connections, only using multi-factor authentication, and only form government-furnished equipment that have full disk encryption. The user list is reviewed on regular basis, and users are removed when they leave the organization or change positions. There are controls in place to monitor, review, and prevent unusual and unauthorized IAST access.

The risk of mishandling or misuse of PII is mitigated through a series of requirements for all IAST system administrators and users:

- IAST system administrators are subject to background checks;
- Prior to gaining system access with elevated privileges, system administrators and users are required to sign a Rules of Behavior which governs their actions; and
- System administrators and users are required to complete required annual security and privacy training.