Privacy Impact Assessment (PIA)

for the

Office of Inspector General Management Information System (OIG MIS)

May 11, 2020

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

Contact Point

Contact Person/Title: Hui Yang / OIG ISSO
Contact Email: Hui.Yang@ed.gov

System Owner

Name/Title: Robert Mancuso / OIG ITACCI AIG
Principal Office: Office of Inspector General

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 OIG MIS does not collect any information directly from individuals, but rather it hosts a file server which may store PII obtained by OIG staff in the course of carrying out the operations and work of the OIG.

The Office of Inspector General (OIG) is an independent entity within the U.S. Department of Education (ED) responsible for identifying fraud, waste, abuse, and criminal activity involving ED funds, programs, and operations. OIG conducts independent audits and other reviews and criminal and civil investigations, recommends actions to address systemic weaknesses and improve ED programs and operations, and changes needed in Federal laws and regulations.

The OIG Management Information System (MIS) hosts a file server which contains records from various applications related to the management of files within OIG such as the Counsel Tracking System (CTS) and the Evidence Tracker. OIG counsel staff utilize the CTS to track and manage tasks, assignments and other essential information to the agency's legal mission in an orderly, systematic and accurate manner. OIG investigators utilize the Evidence Tracker application to track the chain of custody of evidence collected.

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

PII may be obtained by auditors and investigators and maintained in MIS to conduct, supervise, and coordinate audits relating to Department programs and operations as required by the IG Act. Audit objectives frequently require that auditors and investigators examine whether recipients of Federal funds complied with expenditure, use, and disbursement requirements and PII may be present in pieces of evidence. The nature and amount of PII maintained varies by the objective and topic of the audit but

[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

OIG makes every effort to avoid collecting PII.

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

Currently Operating System

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

Updated PIA

1.5. 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.

Inspector General Act of 1978, as amended, 5 U.S.C. Appendix § 6(a) (The Inspector General Act) authorizes the Inspector General to have access to all records, reports, audits, reviews, documents papers, recommendations, or other material available to the applicable establishment which relate to programs and operations with respect to which the Inspector General has responsibilities under the Act.

SORN

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

Yes

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

☐ N/A

Investigative Files of the Inspector General (18-10-01) last fully published in the Federal Register on June 26, 2003 at 68 FR 38153, altered on June 14, 2010 at 75 FR 33608, and again on August 20, 2012 at 77 FR 50091.

Non-Federal Auditor Referral, Suspension, and Debarment File last fully published in the Federal Register on June 4, 1999 at 64 FR 30155 and corrected on December 27, 1999 at 64 FR 72406.

Hotline Complaint Files of the Inspector General last fully published in the Federal Register on June 4, 1999 at 64 FR 30157, corrected on December 27, 1999 at 64 FR 72407 and amended on July 12, 2010 at 75 FR 39669.

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

☑ N/A

Click here to enter text.

Records Management

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

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.

Ed 270 Program Management files- Electronic Information Systems Item 4 (Office of Inspector General Management (OIG) Information System (MIS)Master Data files. Temporary Cut off files annually Destroy/delete 5 years after file cutoff. NARA Job Number N1-441-10-001(1A4).

[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

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.

MIS may store, maintain, and use name, email address, phone number, date of birth, and Social Security number (SSN) of Federal employees, contractors, or members of the public who are necessary in the success of reaching an audit's objective. Additional elements that would specifically relate to the nature of the audit or investigation could include information related to an individual's finances, income, education or other area related to an audit's objective.

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

Yes

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

Any PII maintained in MIS will come from an OIG auditor or investigator who obtains it from a source. During the course of an audit or investigation, during which PII may be intentionally or unintentionally obtained, PII may be collected from a variety of sources including Department of Education records, institutions of higher education, financial institutions, Federal State or local records, interviews with witnesses, documents and other material furnished by nongovernmental sources, State licensing boards, professional organizations, employees of Federal state or local agencies, members of the public, officers and employees of non-governmental organizations involved with or have a knowledge of Department programs, contracts, or funds.

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 collected through investigations and audits by investigators and auditors which can include oral interviews, paper or electronic documents, searches on public facing websites, or emails. Auditors and investigators will upload all collected evidence containing PII within the MIS electronic boundary.

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?

The validity of any PII or other evidence collected is critical to the functions of OIG and the responsibility of auditors and investigators. Through the course of an audit or investigation, PII would be validated across the different sources of evidence by the auditor or investigator handing the case. The purpose of an investigation would be to identify inconsistencies.

Use

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

PII collected during the conduct of audits are in instances primarily where individual records are tracked using PII data as a unique identifier. Collecting PII is critical to audit work in any case where a review of individual-level data is required by the audit objective.

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

3.8. 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.

No

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

☐ N/A

MIS may maintain SSNs which are obtained by auditors and investigators in the course of linking records across various sources of evidence so they can retrieve them for audit and investigative purposes.

The use of SSNs is solely to determine compliance with Federal requirements consistent with OIG objectives. The maintenance of SSNs is limited whenever possible however it is impossible to avoid collecting them as long as the information systems or programs that the OIG audits or investigates use them for identification purposes.

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

☑ N/A

Click here to enter text.

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.

OIG MIS does not collect PII directly from individuals so the system does not provide notice to individuals.

Additionally, MIS contains records that are maintained in systems of records which are exempt from requirements of the Privacy Act. Please refer to the SORNs referenced in 2.2.1 for more 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?

OIG does not provide, at that time, an opportunity for individuals to consent to use of their PII. The auditees may or may not provide such notice or opportunities when they initially collect that information for program or other purposes however, such audits and access to information is mandated under the IG Act.

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?

No

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.

Yes

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

☐ N/A

OIG may share information with all other law enforcement agencies at the local, state, and Federal level including but not limited to the Federal Bureau of Investigations and the U.S. Attorney's office. OIG may also share PII with the Government Accountability Office (GAO), Council of the Inspectors General on Integrity and Efficiency (CIGIE), and other standard setting organizations. Additionally, pursuant to a routine use published in the SORN entitled "Investigative Files of the Inspector General" PII may be disclosed to public and private entities during the course of an investigation.

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

☐ N/A

In many investigations, the subject violator has committed other violations which may fall under the jurisdiction of other law enforcement agencies. In this regard, the auditor or investigator will share information with the appropriate agency in order to ensure that noted criminal, civil, or administrative violations or weaknesses are addressed.
The OIG may share information with the GAO, CIGIE, and other standard setting organizations for the purposes of required peer review.
The OIG may share information with public and private entities for the purposes of obtaining additional information in the course of an audit or investigation.

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

[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.

Yes

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

☐ N/A

Information is always shared in a secure electronic fashion which at a minimum includes encrypting the data with a password that meets our internal OIG password policies. In limited situations, OIG may choose to hand - carry hard copy documents or utilize the signature required, overnight mail to transmit any documents that are shared.

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

Yes

6. Redress

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

Individuals are not allowed to access their own information because the information is obtained for the purpose of conducting audits and investigations. The information maintained in OIG MIS is covered under System of Records Notices that the Department has claimed exemptions from the Privacy Act. Please see 34 CFR 5b.11(b) for more information.

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

Individuals are not allowed to access their own information because the information is obtained for the purpose of conducting audits and investigations. The information maintained in OIG MIS is covered under System of Records Notices that the Department has claimed exemptions from the Privacy Act. Please see 34 CFR 5b.11(b) for more information.

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

Information regarding the record access and amendment exemptions can be found at 34 CFR 5b.11 and in the SORNs listed in question 2.2.1. .

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?

Only authorized and approved users have access to MIS. Access is extremely limited and controlled utilizing multifactor authentication for all users. Access can only be gained by using the ED internal networks and employees and contractors can only gain access to the network after completed an annual cybersecurity and privacy training. MIS is developed and maintained by ED contractors and is housed within a secure and controlled facility. Access to the computer lab is limited to authorized ED personnel only. The general public does not have access to MIS. MIS data is encrypted while in transit and at rest. Monitoring controls are in place to determine if there is unauthorized accessor downloading of the data.

Additionally, there are common controls implemented on the OIG MIS to safeguard information. These controls are provided by the Department and include, Intrusion

Prevention and Intrusion Detections Systems (IPS/IDS), Anti-virus (AV) software on workstations and servers and Data Loss Prevention (DLP) software.

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.

This is a FISMA reportable system and is reviewed annually and as needed when significant changes to the system occur. As part of the Department's continuous monitoring program, MIS is expected to review and renew their Authorization to Operate on a regular basis. This process includes audits of the implemented security and privacy controls by independent assessors. Findings from these audits produce Plans of Actions and Milestones (POAMs) for OIG to remediate. Self-assessments are also conducted on a annual basis as are incident response and contingency plan testing. On a more frequent basis, scans are performed to check for vulnerabilities and available patches.

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?

Each year, OIG selects a random sample of projects to evaluate for compliance with government auditing standards and additional OIG procedures. The evaluation determines if OIG is collecting information in accordance with and for the purposes stated in this PIA. In addition, MIS is subjected to continuous security monitoring and annual security self-assessment.

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 and use of the information maintained in MIS. To mitigate these risks all users are approved and sign an agreement as to the proper use of the data.. MIS access is from internal network connections only using multi-factor authentication. The user list is reviewed annually, and users are removed when they leave the organization or change positions. There are controls in place to monitor and review when unusual activity occurs.