Privacy Impact Assessment (PIA)
for the

ITACCI Laboratory Network (ITACCINet)
June 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: Scott Oglesby
Contact Email: scott.oglesby@ed.gov

System Owner

Name/Title: Robert Mancuso, Assistant IG for ITACCI
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 mission of the Department of Education (ED) Office of the Inspector General (OIG), is to promote the efficient and effective use of taxpayer dollars in support of American education by providing independent and objective assistance to the Congress and the Secretary in assuring continuous improvement in program delivery, effectiveness, and integrity. The Information Technology, Audits and Computer Crime Investigations (ITACCI) component of the OIG, established the ITACCI Laboratory Network (ITACCINet) to provide an independent environment for its mission, independent of the ED network and systems. ITACCINet is a general support system (GSS) for investigative support that provides centralized user and computer object management, centralized file storage, content management services, network printing, and internet connectivity through a Trusted Internet Connection (TIC)-compliant managed trusted internet protocol services (MTIPS) circuit. The IG Act of 1978 (as amended), provides the OIG the authority to operate as a "separate agency," and as such, we have the authority to maintain an independent network to support the OIG mission, whose requirements and needs are different from the Department. Further, the OIG requires an environment that is maintained and administered by OIG personnel, with appropriate clearances, and not a contractor owned, contractor operated environment.

The information maintained within this system is limited to information that OIG has legal authorization to collect and maintain as part of its responsibility to conduct, supervise, and coordinate audits and investigations of Department programs, operations, grantees, contractors, and associated personnel to recognize and mitigate fraud, waste, and abuse.

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

While ITACCINet does not purposefully collect PII, there may be PII incidentally included in digital evidence records obtained through search warrants and investigative data collection that are stored on the system. Digital evidence is defined as information and data of value to an investigation that is stored on, received or transmitted by an

[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, SSN, 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

electronic device.[2] Digital evidence, such as forensic images of computer hard drives, may be obtained by criminal investigators from external sources or from internal Department and OIG systems for law enforcement purposes. The scope of digital evidence maintained by investigators is unique to every case and includes what the agent deems relevant to the case. Therefore, the digital evidence varies depending on the case being investigated.

ITACCINet does not have interconnections with other systems for sharing of digital evidence.

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?

New PIA

The Privacy Safeguards Office reviewed the ITACCINet Privacy Threshold Analysis and system architecture and determined that the PII present in digital evidence now maintained on this system warranted a 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.

[2] Electronic CSI, A Guide for First Responders, 2nd edition, National Institute of Justice, April 2008

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.

5 U.S.C. Appendix § 6(f) (The Inspector General Act) - Each Inspector General, any Assistant Inspector General for Investigations under such an Inspector General, and any special agent supervised by such an Assistant Inspector General may be authorized by the Attorney General to seek and execute warrants for arrest, search of a premises, or seizure of evidence issued under the authority of the United States upon probable cause to believe that a violation has been committed.

5a U.S.C. Appendix § 2(1) (The Inspector General Act) - Authorizes the Offices of Inspector General to conduct and supervise audits and investigations relating to the programs and operations of their establishments and agencies.

Inspector General Act of 1978, as amended, 5 U.S.C. App. § 3 (2012 & Supp. IV 2016);

DATA Act, Pub. L. No. 113–101, 128 Stat. 1146. (codified as amended in scattered sections of 31 U.S.C.);

Inspector General Empowerment Act (IGEA) of 2016, Pub. L. 114-317, 130 Stat. 1595 (2016).

Federal Rules of Criminal Procedures and Federal Rules of Civil Procedures.

SORN

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

No

The data (queries, searches, or other analyses) stored on ITACCINet do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the network. PII may be incidentally included in digital evidence records obtained through search warrants and investigative data collection.

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

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

While PII is maintained on ITACCI as described in Section 1.2, the information is not retrieved by an identifier. The data (queries, searches, or other analyses) stored do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the network.

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 OIG Technology Crimes Division Policies and Procedures Manual, Chapter 5110, defines the retention policies for records maintained on the ITACCINet system. The ITACCI system only maintains reference copies of records generated for investigations or in response to requests for assistance. All records provided to OIG components (e.g., Investigative Services or Audit Services) will be retained per OIG NARA DISPOSITION AUTHORITY: N1-441-02-1.

At the end of each fiscal year, a review of the status of OIG investigative cases is performed. If a case is closed, the reference copies of records are moved to a designated retention area on the ITACCINet file server. The reference copies are destroyed after a case has been closed 10 years. Digital evidence is retained on ITACCINet until the case

[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

agent receives permission from the prosecuting attorney to destroy the evidence. Upon receipt of that notification, the case agent instructs the evidence custodian to dispose of all appropriate evidence.

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, SSN, etc.) that the system collects, uses, disseminates, or maintains.

ITACCINet does not purposefully collect PII. However, the network may contain PII that may be included incidentally in digital evidence records. PII commonly found on ITACCINet in digital evidence records maintained by this system includes, but may not be limited to, name, date of birth, address, SSN, and email address. These digital evidence records are obtained from relevant sources during investigations for law enforcement purposes.

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

Yes

ITACCINet does not purposefully collect PII. Any PII stored on ITACCINet is the minimum necessary to provide evidence for the investigation for which it was collected.

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

Under the Inspector General Act of 1978, as amended, OIG is authorized to carry out audits and investigations, which can include criminal, civil, and administrative matters. The information maintained within this system is limited to information that OIG has legal authorization to collect and maintain as part of its responsibility to conduct, supervise, and coordinate audits and investigations of ED programs, operations, grantees, contractors, and associated personnel to recognize and mitigate fraud, waste, and abuse.

As part of its audit and investigatory functions, OIG obtains digital evidence through law enforcement mechanisms, such as from search warrants, subpoenas, consent searches, another agency or law enforcement entity, and/or commercial sources (e.g., LexisNexis). This evidence obtained from these sources are digitally stored on ITACCINet, and some of this digital evidence includes PII.

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

Digital evidence may be obtained electronically or digitized from paper as the result of a search warrant, subpoena, consent, or other similar request.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[4] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

The OIG adheres to the standards and principles of the Council of the Inspectors General on Integrity and Efficiency (CIGIE) Quality Standards for Digital Forensics (QSDF). The QSDF address the processes and specialized techniques for gathering, retaining, and analyzing electronically stored information (digital evidence), and reporting the resulting conclusions for investigative purposes.

Following these standards, the OIG ensures digital evidence is not unintentionally altered during or after the acquisition. Methods include:

- Performing appropriate validation testing of acquisition tools.
- The use of hashing algorithms when collecting and authenticating digital evidence.
- Ensuring that personnel handle and store digital evidence in a manner that precludes the inadvertent alteration or destruction of evidence by human action or environmental conditions.
- Ensuring the chain of custody for all digital evidence is maintained.

The data are controlled, maintained, and attested to by OIG personnel that are certified in digital forensic procedures and meet CIGIE standards.

Use

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

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

The information maintained within this system is limited to information that OIG has legal authorization to collect and maintain as part of its responsibility to conduct, supervise, and coordinate audits and investigations of Department programs, operations, grantees, contractors, and associated personnel to recognize and mitigate fraud, waste, and abuse. The PII identified in digital evidence obtained during an investigation may help to identify victims of a crime, perpetrators, or simply provide evidence of a crime.

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 SSNs, 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 SSNs? Note that if the system maintains SSNs but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

Yes

The system does not purposefully collect individual SSNs, but maintains digital files that may include SSNs.

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 information maintained within this system is limited to information that OIG has legal authorization to collect and maintain as part of its responsibility to conduct, supervise, and coordinate audits and investigations of ED programs, operations, grantees, contractors, and associated personnel. SSNs may be identified

during an investigation and analysis of SSNs or other investigative data may help to identify victims, perpetrators, or simply provide evidence of a crime.

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.

Notice is not provided to individuals whose PII is maintained by ITACCINet because the digital evidence that is stored on the system, that may contain PII, is exempted under Exemptions (d)(5) and (j)(2) of the Privacy Act. The digital evidence is compiled in reasonable anticipation of a civil action or proceeding, and the records in the system are compiled during the course of criminal law enforcement proceeding. General notice is provided by this 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

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?

ITACCINet does not purposefully collect PII, but instead maintains digital evidence that may incidentally include PII as part of the digital evidence records. Therefore, individuals do not have the ability to decline to provide information or opt out of their information being maintained.

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.

Yes

5.2. What PII will be shared and with whom?

The OIG may share names, SSNs, dates of birth, addresses, and any other relevant information contained in digital evidence obtained by the OIG with the Department's Federal Student Aid (FSA) if there is an investigation that indicates an individual(s) may be engaged in fraud, or are victims of fraud or abuse. The sharing of this information is for investigative purposes to mitigate risks associated with student accounts that FSA is responsible for managing. Any other type of investigative activities not related to FSA would not and cannot be shared with other offices. This would infringe on the OIG's ability to conduct an independent and objective investigation into an allegation of fraud or abuse.

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

The purpose of sharing PII internally with FSA is to identify victims or perpetrators of fraud or abuse. OIG Technology Crimes Division (TCD) is responsible for investigating information technology (IT) based crimes. TCD's nationwide investigative jurisdiction encompasses any public or private information technology system used in the administration of Department-sourced funds. TCD often collaborates with FSA in regards to cybersecurity incidents at institutions of higher education and allegations of fraud concerning student loan debt relief scams. TCD shares actionable information and data originating from FSA Title IV systems and recipients with FSA and the Department to remediate vulnerabilities within their systems. TCD works closely with the Department and FSA to aggressively pursue those who criminally misuse IT systems, which may require the sharing of PII and investigative intelligence.

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

If PII contained in digital evidence obtained by the OIG identifies the victim or perpetrator of criminal activities, the OIG may share the data with other law enforcement agencies (e.g., Federal Bureau of Investigation (FBI), Assistant U.S. Attorney Offices, Federal State and Local Law Enforcement Agencies, and OIG offices at other Federal agencies).

5.5. What PII will be shared and with whom? List programmatic disclosures only.[5]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☐ N/A

The OIG may share PII, including SSNs, occurring in digital evidence obtained by the OIG with other law enforcement agencies (e.g., FBI, Assistant U.S. Attorney Offices, Federal State and Local Law Enforcement Agencies, and OIG offices at other Federal agencies). The Inspector General Empowerment Act of 2016 (IGEA) exempts certain computerized data comparisons performed by or in coordination with Inspectors General (IGs) from the Computer Matching and Privacy Protection Act's restrictions and requirements (the "CMPPA Exemption"). Specifically, the IGEA added section 6(j)(2) to the Inpector General Act: For purposes of section 552a of title 5, United States Code, or any other provision of law, a computerized comparison of two or more automated Federal systems of records, or a computerized comparison of a Federal system of records with other records or non-Federal records, performed by an Inspector General or by an agency in coordination with an Inspector General in conducting an audit, investigation, inspection, evaluation, or other review authorized under this Act shall not be considered a matching program. The OIG signs specific data use agreements with specific Federal Inspector Generals using Memorandums of Agreement (MOA). In the absence of an MOA, data may still be shared with Federal, state, local, tribal, and foreign law enforcement, counterterrorism, and border security agencies on a case-by-case basis. Data are stored and tracked by case number that is not a personal identifier in accordance with investigative guidelines.

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

☐ N/A

[5] 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 may be shared for prosecutive and investigative purposes. For example, PII may be shared for the purpose of identifying and notifying the victims and/or the perpetrators of criminal activity in a case that is being jointly investigated by the OIG and another law enforcement agency.

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

Information is always shared in a secure fashion that employs approved encryption techniques. For example, National Institute of Standards and Technology (NIST) FIPS 140-2 certified portable harddrive enclosures with hardware-based encryption are utilized to share data with external entities. The data can only be decrypted with a hardware encryption key that is stored apart from the harddrive enclosure.

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

No

The IGEA exempts from the definition of a matching program any computerized data comparisons of Federal systems of records, or of a Federal system of records with other records (including non-Federal records) performed by or in coordination with an OIG so long as the match is performed in connection with an audit, investigation, inspection, evaluation, or other review authorized under the Inspector General Act. As a result, OIGs can engage in matching without adhering to the Computer Matching and Privacy Protection Act's various restrictions and requirements discussed above. Thus, OIGs are no longer required to enter into CMAs prior to receiving or disclosing records that will be used for matching purposes.

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?

ITACCINet is a law enforcement system and is exempt from the notification, access, and amendment procedures of the Privacy Act. The information on this network consists of investigatory material compiled for law enforcement purposes. This system is exempt from certain provisions of the Privacy Act including the provisions regarding access to records. See 5 U.S.C. § 552a(k)(2) and 34 C.F.R. § 5b.11(c)(1). However, OIG will consider individual requests to determine whether or not information may be released. Individuals seeking notification of and access to any OIG record about themselves can file a Freedom of Information Act (FOIA) request with the Department.

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

The system is a law enforcement system and is exempt from many of the provisions of the Privacy Act. OIG will consider requests to determine whether information can be released. Request should be submitted to:

U.S. Department of Education
Office of the Executive Secretariat
FOIA Service Center
400 Maryland Avenue, SW, LBJ 7W106A
Washington, DC 20202-4536
ATTN: FOIA Public Liaison

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

No individual notification of procedures for correcting records is provided. ITACCINet contains investigatory material compiled for law enforcement purposes and is exempt from the amendment provisions of the Privacy Act. Notification to individuals that they are or have been the subject of a law enforcement investigation would undermine the performance of the law enforcement mission of OIG. However, requests for redress should be directed the FOIA Service Center, listed in Section 6.2.

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?

ITACCI has received an Authorization to Operate and has put in place all required controls at the moderate categorization level under NIST standards.

Only authorized and approved users have access to ITACCINet. Network access to the ITACCI system is strictly limited to ITACCI and OIG personnel, unless approved by the ITACCI System Owner (e.g., law enforcement personnel from another agency or OIG contractors). All users must be approved for access through a User Account Request system, have a 6C security clearance, and sign an rules of behavior agreement.

ITACCINet is operated and maintained by OIG personnel and is housed within a secure and controlled facility. Access to the computer lab is limited to authorized OIG personnel only. The general public does not have access to ITACCINet.
Monitoring controls are in place to determine if there is unauthorized access and/or changes on the system.

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 ITACCI security team conducts a yearly self-assessment of selected security controls. All applicable NIST security controls applicable to a moderate system are assessed within a three-year cycle. A yearly report of the results is written and any risks that are identified are noted and tracked for correction. The yearly report is presented to the system owner and authorizing official. The results are reviewed with them and any required corrective actions are discussed. An independent assessment is performed on ITACCINet every three years.

Additional monitoring, testing, and evaluations are conducted on a regular basis to ensure that ITACCINet security controls are in place and effectively safeguarding PII. These include:

- Real-time file integrity and change monitoring
- File hashes are calculated and documented for investigative evidence; the integrity of evidence is verified before and after forensic analysis
- Privileged user accounts are reviewed and validated quarterly
- Non-privileged user accounts and access are reviewed and validated annually
- Antivirus scanning and reporting
- Weekly vulnerability scanning
- Security event detection and alerting
- Periodic log reviews

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?

In accordance with FISMA, an annual self assessment of security countols is performed on ITACCINet and an independent assessment is performed every three years. All ITACCI users sign a user agreement that indicates the proper use of the system and the consequences of not following the rules of behavior. This agreement require users to "[i]mmediately notify your system administrator, ISSO, and supervisor of any and all network or system security incidents. This is especially important for incidents involving personally identifiable information (PII), which must be reported to US-CERT within one hour of discovering the incident." Privileged user accounts are reviewed quarterly, and non-privileged user accounts are reviewed annually to ensure that only authorized OIG employees have access. Security groups have been established to control access to shares and/or folders containing PII. Firewalls segment internal ITACCI systems and further restrict access to systems containing PII.

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?

The primary privacy risks are unauthorized access and disclosure of PII.

All ITACCINet data are protected by the technical, operational, and management security controls identified, defined, and implemented using NIST 800-53 and Department directives and guidelines. Compliance with these controls is monitored and enforced by a full-time Information System Security Officer (ISSO) and governed by Department and OIG policies.

All security controls are tracked and monitored in the ITACCINet System Security Plan (SSP). All persons with ITACCINet access must have a minimum 6C, High Risk, security clearance. All ITACCI personnel must also sign the ITACCINet Rules of Behavior agreement, complete the Department Cybersecurity Awareness and Training, and be approved by ITACCI management prior to being granted access to ITACCINet. Furthermore, ITACCINet employs strict user controls that limit the access and functions that individual users may perform after access is granted.