Privacy Impact Assessment (PIA)
for the

Office of the Inspector General Local Area Network (OIG LAN)

Feb 27, 2019

This PIA was originally approved on Aug 6, 2008 and reviewed on Feb 27, 2019 by the system owner certifying the information contained here is current and up to date.

Contact Point

Contact Person/Title: Hui Yang, OIG ISSO

Contact Email: Hui.Yang@ed.gov

System Owner

Name/Title: David A. Morris, Assistant Inspector General for Management Services

Program Office: Office of Inspector General (OIG)

Please submit completed Privacy Impact Assessments to the Privacy Safeguards Division 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.***

All text responses are limited to 1,500 characters. If you require more space, please contact the Privacy Safeguards Team.

1. Introduction

1.1 Describe the system including the system name, system acronym, and a brief description of the major functions.

The Office of the Inspector General Local Area Network (OIG LAN) is a General Support System (GSS) that provides network infrastructure for the OIG Intranet and the Management Information System (MIS). These major applications contain OIG staff user data files, various OIG databases and applications which may contain privacy, proprietary, financial, and audit data.

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. We conduct independent audits and other reviews and criminal and civil investigations, recommend actions to address systemic weaknesses and improve ED programs and operations, and changes needed in Federal laws and regulations.

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

The OIG LAN 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.

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. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf

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? If this is an update, please include the publication date of the original.

Updated PIA Original Publication Date: 08/06/2008

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

Contractor

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?

5 U.S.C. App., Inspector General Act of 1978, as amended. Pub. L. 95-452 (Dec. 16, 2016).

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? Please answer **YES** or **NO**.

No

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

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 Does a records retention schedule, approved by the National Archives and Records Administration (NARA), exist for the records contained in this system? If yes, please provide the NARA schedule number.

Yes, OIG manages records in accordance with NARA's General Records Part 16 – Office of Inspector General Records (https://www2.ed.gov/policy/gen/guid/fra/part-16sch.pdf). The NARA disposition authority is N1-441-02-1.

[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? Please answer **YES** or **NO**.

Yes

3. Characterization and Use of Information

Collection

3.1 List the specific personal information data elements (e.g., name, email, address, phone number, date of birth, Social Security Number, etc.) that the system collects, uses, disseminates, or maintains.

OIG LAN does not collect PII from individuals. However, it may store PII obtained by OIG staff in the course of carrying out the work of the OIG. Items include: Auditees and investigation case related person's names, addresses, SSNs, phone numbers.

3.2 Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2? Please answer **YES** or **NO**.

Yes

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

They system may store PII obtained by OIG staff in the course of carrying out the work of OIG. Sources include: auditees, investigation/case subjects and witnesses.

3.4 How is the information collected from stated sources (paper form, web page, database, etc.)?

Paper and electronic documents are collected and stored in databases, folders, and as scanned images.

3.5 How is this information validated or confirmed?[3]

Auditors and investigators validate the information they obtained through auditees, investigation/case subjects and witnesses.

[3] Examples include form filling, account verification, etc.

Use

3.6 Describe how and why the system uses the information to achieve the purpose stated in Question 1.2 above.

OIG LAN provides network infrastructure for major applications that staff use to manage and track work. This system does not collect PII, rather it is a general support system for the management of such information used by OIG staff in the conduct of carrying out the work of OIG.

3.7 Is the project using information for testing a system or for training/research purposes? Please answer YES or NO.

No

3.7.1 ☒ N/A If the above answer is **YES,** what controls are in place to minimize the risk and protect the data?

3.8 Does the system use "live" PII for the development or testing of another system? Please answer YES or NO.

No

3.8.1 ☒ N/A If the above answer is **YES,** please explain.

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 system collect Social Security Numbers? Please answer **YES** or **NO**.

No

3.9.1 ☐ N/A If the above answer is **YES,** explain the purpose for its collection, and how the SSN will be used. *Please note if the system collects SSNs, the PIA will require a signature by the Assistant Secretary or equivalent.*

OIG does not collect SSNs, however, it does store them on the occasion it is included in the files from OIG staff. Although not requested or required, the SSN will be sufficiently safeguarded.

3.10 ☒ N/A Specify any alternatives considered in the collection of SSN and why the alternatives were not selected.

4. Notice

4.1 How does the system provide individuals notice about the collection of PII prior to the collection of information (i.e. written Privacy Act notice, link to a privacy policy, etc.)? If notice is not provided, explain why not.

This system does not collect PII directly from individuals but from different entities (i.e., student information through FSA and/or a fraud related bank transaction records through financial institutes). It is their responsibility to provide notice to the individual about the collection of their personal information.

OIG LAN's privacy policy can be found: https://www2.ed.gov/about/offices/list/oig/warning.html

4.2 ☒ N/A Provide the text of the notice, or the link to the webpage where the notice is posted.

4.3 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Individuals' consent is not required for the PII obtained through audits and investigations.

5. Information Sharing

Internal

5.1 Will information be shared internally with other ED organizations? Please answer **YES** or **NO**. If the answer is **NO**, please skip to Question 5.4.

Yes

5.2 ☐ N/A What information will be shared and with whom?

Any of the information maintained on OIG LAN may be shared with other Department offices or staff on a "need to know" basis.

5.3 ☐ N/A What is the purpose for sharing the specified information with the specified internal organizations? Does this purpose align with the stated purpose in Question 1.2 above?

Information maintained on OIG LAN may be shared with other Department offices or staff on a "need to know" basis as necessary to carry out the work of the OIG including for purposes of audit management, tracking and resolution; tracking and responding to correspondence; and managing OIG's budget, training and human resources responsibilities.

External

5.4 Will the information contained in the system be shared with external entities (e.g. another agency, school district, etc.)? Please answer **YES** or **NO**. If the answer is **NO**, please skip to Question 5.8.

Yes

5.5 ☐ N/A What information will be shared and with whom? Note: If you are sharing Social Security Numbers, externally, please specify to whom and for what purpose.

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.

5.6 ☐ N/A What is the purpose for sharing the specified information with the specified external organizations? Does this purpose align with the stated purpose in Question 1.2 above?

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 Special Agent will share information with the appropriate agency in order to ensure that noted criminal, civil, or administrative violations or weaknesses are addressed. The information is transferred via paper format or transmitted electronically using password-protected email or other ED approved method for transmitting PII. 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.

5.7 ☐ N/A How is the information shared and used by the external entity?

As necessary, the information may be shared using various methods such as, emails, hard copies, and/or CDROMs. Information is only shared externally as necessary to carry out the work of the OIG. External entities could use the information to understand or object to an OIG finding or recommendation.

5.8 ☐ N/A Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU) or other type of approved sharing agreement with another agency? Please answer **YES** or **NO**.

No

5.9 ☐ N/A Does the project place limitation on re-disclosure? Please answer **YES** or **NO**.

No

6. Redress[4]

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

Individuals are not allowed to access their own information. The information is obtained for the purpose of conducting audits and investigations.

[4] If the system has a System of Records Notice (SORN), please provide a link to the SORN in Question 6.1 and proceed to Section 7 - Safeguards.

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 information; therefore, there are no procedures to allow individuals to correct inaccurate or erroneous information.

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

Individuals are not allowed to access their information; therefore, there are no procedures to allow individuals to correct inaccurate or erroneous 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 CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible? Please answer **YES** or **NO**.

Yes

7.2 What procedures or access controls are in place to determine which users may access the information and how does the project determine who has access?

Access to audit tracking information and projects that may contain PII is assigned by the OIG Strategic Planning and Administration Resolution (SPAR) division. Access to human resources information that contains PII is controlled by the OIG Management Services division. In both cases, access is controlled via Department provided user accounts and security groups. Access to all applications within OIG LAN is controlled by specific accounts, assigned roles and respective permissions. List of users are viewable within system.

7.3 What administrative, technical, and physical safeguards are in place to protect the information?

OIG LAN authenticates user access primarily through Department provided authentication and directory services (including user accounts and security groups). The SPAR and Management Services divisions manage access with Department provided services to provide user accounts access to files. To access files a user must be added to the appropriate security group. Access is limited to users with need-to-know. Those users with need-to-know are added to the "security group" referred in the statement in order to gain access to the information.

7.4 Is an Authority to Operate (ATO) required? Please answer **YES** or **NO**.

Yes

7.5 Is the system able to provide account of any disclosures made? Please answer **YES** or **NO**.

Yes

7.6 Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by federal law and policy? Please answer YES or NO.

Yes

7.7 Has a risk assessment been conducted where appropriate security controls to protect against that risk been identified and implemented? Please answer YES or NO.

Yes

7.8 Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the controls continue to work properly at safeguarding the information.

This is a FISMA reportable system and is reviewed annually or as needed when significant changes to the system occur. In addition to previously described file permission and user authentication controls, there are common controls implemented on the OIG LAN 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, Data Loss Prevention (DLP) software, and data corruption prevention software. Additionally all Department users are required to take annual security training which includes handling sensitive data such as PII.

8. Auditing and Accountability

8.1 How does the system owner ensure that the information 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.

8.2 What are the privacy risks associated with this system and how are those risks mitigated?

Risks that might exist are files containing PII might become compromised. This risk is reduced by a combination of common controls discussed in 7.8 as well as limiting access to files to only those that need access via user accounts and security groups. IPS/IDS reduces the risk by preventing unauthorized access on the network and detecting when unauthorized attempts to access the network are being made.

AV software is used to reduce the risk of malicious software from attacking and compromising systems which could allow the exfiltration of data. DLP software is used to reduce the risk of unauthorized exfiltration of PII. Lastly all users are required to take annual security training which includes handling sensitive data. This reduces the risk of exposure that may occur if automated software defenses do not detect an unauthorized attempt to access data such a phishing attempt.