



**Privacy Impact Assessment (PIA)**  
for the

**Office of Inspector General CMS**  
**November 23, 2021**

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

**Contact Point**

**Contact Person/Title:** Carrie Jackson  
**Contact Email:** carrie.jackson@ed.gov

**System Owner**

**Name/Title:** Robert D. 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](mailto: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.

Office of Inspector General (OIG) Case Management System eCase (CMS) is a FedRAMP-authorized Software as a Service (SaaS) application that enables OIG to: store and manage records of investigations, hotline complaints, and audit records; track information related to managing OIG's investigations and audit functions; and to produce related reports. An audit is a review governed by applicable standards, and based on objectives (i.e., what the audit seeks to find) that may result in recommendations to the auditee (e.g., whether an agency component's policies and procedures for overseeing contractors are effective and, if not, auditors make recommendations to improve them). An investigation is a fact-finding exercise that may, depending on the facts, result in referrals for criminal, civil, or administrative action.

OIG CMS eCase is hosted online by a FedRAMP-authorized SaaS cloud service provider (CSP). The system is divided into two separate applications – the Audits Application and the Investigations Application – each of which has its own login authentication and credentials.

OIG users must login to the U.S. Department of Education (Department) network using a government-issued personal identity verification (PIV) card and personal identification number (PIN) or an alternate Department-approved multi-factor authentication credential to access the OIG CMS eCase login portal. The system then requires a user to log in with a unique username and password. The system has front-end web applications and back-end databases. There is a public-facing portal that collects information that populates the Investigations Application. The system is only accessible by OIG staff, through the Department's virtual private network (VPN), after receiving approval from OIG administrators. Administrators issue username/passwords and assign the user with appropriate permissions. There is a public-facing portal in the Investigations Application where complainants can provide details about their allegations, but they cannot access the system.

The Investigations Application maintains records related to OIG criminal, civil, and administrative investigations. This application also maintains records of OIG investigators' time and expense reporting, training, and duty-related equipment assigned to OIG investigators.

The Audits Application maintains records of audit and project management, performance milestone tracking, finding and recommendation management, audit performance management, non-Federal auditor referral, suspension and debarment files, and audit/project reporting. This application also tracks OIG auditors' time and expense reporting and training. There is no public-facing element of the Audits Application.

- 1.2. Describe the purpose for which the personally identifiable information (PII)<sup>1</sup> is collected, used, maintained or shared.

### System Users

Department OIG employees' and contractors' information is collected (as outlined in 3.1) for use of the system.

### Audit Application

In response to an audit, Auditors may request records from an auditee that include PII that the auditee has collected or has been provided, and we collect those records from the auditee if the PII is necessary to meet the audit's objective. OIG uses PII in the records obtained from auditees and maintained in the CMS Audit Application to assess auditee compliance or performance relative to audit objectives. OIG shares Audit Application records, which may include PII, during its triennial peer review, if those records were originally provided by the auditee.

### Investigations Application

In the Investigations Application, PII is collected, used, maintained, and shared to conduct criminal, civil, or administrative investigations involving Department programs and operations. OIG Special Agents rely on PII to accurately identify witnesses, victims, and subjects throughout the course of an investigation. PII is shared with law enforcement, prosecutors, and other Department officials when necessary for criminal, civil, or administrative actions.

---

<sup>1</sup> 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](#)

1.3. 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

This is an update to an existing PIA. The previous PIA did not include records for the Audit Application. The previous PIA for the Investigations Application was approved in 2017.

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

Contractor

The contractor provides FedRAMP-authorized SaaS application.

1.5.1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

N/A

Yes

## 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.

5 U.S.C. App. § 4(a)(1) and 6(a) (Inspector General Act of 1978, as amended) authorizes the Inspector General to conduct, supervise, and coordinate civil and criminal investigations and audits relating to the programs and operations of the Department and to have access to all documents or other material available to the Department which relate to its programs and operations.

SORN

FY 2020

**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)).<sup>2</sup> Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

N/A

The following SORNs apply to records in the Investigations and Audit Applications that are retrieved by name or other personal identifier:

The Investigative Files of the Inspector General SORN (18-10-01), 86 FR 54171 (September 30, 2021).

Training records: Government-wide Personnel SORN (OPM GOVT-1), 77 FR 73694, (December 11, 2012).

Non-Federal Auditor Referral, Suspension, and Debarment File SORN (18-10-03), 64 FR 30106 (June 4, 1999) and 64 FR 72384 (December 27, 1999).

**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

## Records Management

**If you do not know your records schedule, please consult with your records liaison or send an email to [RMHelp@ed.gov](mailto:RMHelp@ed.gov)**

---

<sup>2</sup> 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>

- 2.3. 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.

#### Audit Application

Audit Records - disposition schedule found at [https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-education/rg-0441/n1-441-02-001\\_sf115.pdf](https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-education/rg-0441/n1-441-02-001_sf115.pdf)

Time and Expense & Training Records - disposition schedule found at [https://www.archives.gov/files/records-mgmt/rcs/schedules/general-records-schedules/daa-grs-2016-0016\\_sf115.pdf](https://www.archives.gov/files/records-mgmt/rcs/schedules/general-records-schedules/daa-grs-2016-0016_sf115.pdf)

#### Investigations Application

Hotline Records of the Inspector General - disposition schedule found at [https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-education/rg-0441/n1-441-02-001\\_sf115.pdf](https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-education/rg-0441/n1-441-02-001_sf115.pdf)

Investigation Records of the Inspector General - disposition schedule found at [https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-education/rg-0441/n1-441-02-001\\_sf115.pdf](https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-education/rg-0441/n1-441-02-001_sf115.pdf)

#### Time and Expense, Training Records, Inventory Records:

[https://www.archives.gov/files/records-mgmt/rcs/schedules/general-records-schedules/daa-grs-2016-0016\\_sf115.pdf](https://www.archives.gov/files/records-mgmt/rcs/schedules/general-records-schedules/daa-grs-2016-0016_sf115.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.

## System Users

Information collected about system users (OIG staff) includes name and work-related details such as username, job grade, phone number, email, work locations, and job title, time and expense and inventory records.

## Audit Application

When auditees provide records containing PII to the OIG as described in section 1.2, the records may include first names, last names, Social Security numbers (SSN), dates of birth (DOB), email addresses, mailing addresses, phone numbers, academic records, financial records, attendance records, institutional records, and/or Free Application for Federal Student Aid (FAFSA) data. The actual data elements will vary depending on the records provided by the auditee (e.g., school, local education agency, institution of higher education, state department of education, student loan guarantor, student financial aid lender, U.S. Department of Education, etc.). Any personal information collected is unstructured data in files provided by the auditee. Generally, the PII in these records includes PII of students enrolled at a primary or secondary institution. This PII can include name, phone number, address, DOB, academic records, financial records, attendance records, and/or personal details.

## Investigations Application

Elements of PII collected and maintained in the Investigations Application within CMS are: name, DOB, race, ethnicity, place of birth, home address, home phone, personal email, medical information, alias, and personal identification-such as SSN, passport number, driver's license number, taxpayer identification number, financial account, credit card number, street address, email address, and personal characteristics including but not limited to: photographic image, fingerprints, handwriting, biometric data. Race, age, and ethnicity are required for subjects and victims for National Incident-Based Reporting System (NIBRS) reporting.

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

Yes

Investigations Application: The Investigative Files of the Inspector General are exempt from the requirement to maintain only such information about an individual as is relevant and necessary to accomplish an agency purpose.

Audits Application: Audit supervisors determine the amount of PII required to meet audit objectives. Audit personnel are generally discouraged from using PII in audits unless it is necessary to meet audit objectives

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

#### **Audit Application**

Sources of PII include various Department information systems which are populated by data submitted by schools, local educational agencies, state education agencies, institutions of higher education, student financial aid lenders, student loan guarantors, and grant recipients. OIG may also get records that contain PII from auditees which include the Department and Department grantees, subgrantees, or other entities who receive Department funds.

#### **Investigations Application**

PII is obtained from various sources. The most common sources of PII are employees, grantees, sub-grantees, contractors, students, program participants' family members, schools, or others with knowledge of fraud, waste, or abuse in government programs.

PII originates from several sources such as: (1) personal interviews and investigative activities, (2) the Hotline website that enables public submission of complaints of fraud, waste, and abuse using an online standardized form, (3) telephone call-in, (4) paper form through mail or delivery service, (5) fax, (6) in-person walk-in complaint, (7) National Crime information Center/National Law Enforcement Telecommunication Service (NCIC/NLETS) databases, and (8) National Student Loan Data System (NSLDS) or other Department student aid 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.)?

#### **Audit Application**

During the course of an audit, OIG will request information from auditees. The auditees will then provide the information to OIG, often by submitting files, such as email, text (.txt), comma separated value (.csv), Acrobat (.pdf), Word (.docx), Excel (.xlsx), or other similar files that an auditee may use.

#### **Investigations Application**

In the Investigations Application, PII originates from several sources, such as: (1) personal interviews and investigative activities, (2) the Hotline website that enables public submissions of complaints of fraud, waste, and abuse using an on-line standardized form, (3) telephone call-in, (4) paper form through mail or delivery service, (5) fax, (6) in-person walk in complaint,



(7) National Crime information Center/National Law Enforcement Telecommunication Service (NCIC/NLETS) databases, and (8) National Student LoanData System (NSLDS) or other Department student aid systems.

- 3.5.** How is the PII validated or confirmed to ensure the integrity of the information collected?<sup>3</sup>  
Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

### Audit Application

The rigor and depth of OIG's PII validation in audits and inspections is required by Government Auditing Standards to be appropriate to the scope of the audit. The level of data validation may vary depending on the nature of a particular review. Data validation is necessary when the information itself is intended to materially support conclusions regarding the audit's objectives. Typically, the integrity of data is validated by processes such as (1) gaining an understanding of controls relating to the data itself through interviews, policy reviews, and observation; (2) use of corroborating evidence - for example, tracing a sample of records back to original sources or comparing data from different systems; and/or (3) testing of the data itself for things like completeness, duplication, outliers, or expected relationships.

Data are obtained as of a point in time to support conclusions relevant to the project's scope period. As such, continuous validation of changing data over time is not applicable to how the work is performed.

### Investigations Application

Investigations comply with the Council for the Inspectors General on Integrity and Efficiency (CIGIE) Quality Standards for Investigation (QSI). The QSIs address investigator qualifications, independence, and due professional care. Managers review the case file field entries, uploaded investigative documents, and indexes at case opening, quarterly intervals, and case closing to confirm accuracy of information, to include PII, entered in the system.

## Use

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

---

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

### Audit Application

OIG uses PII collected in audits and inspections to evaluate student and institutional eligibility for programs, funds, or services provided directly or indirectly through the U.S. Department of Education. OIG also audits and inspects Department operations and may request that the auditee provide records containing PII when the scope of the audit requires it.

### Investigations Application

PII is used for law enforcement purposes, including the investigation and criminal prosecution of fraud, waste, and abuse of Federal funds. CMS is used to account for processes and tracks information gathered during an investigation in order to resolve matters concerning the possible existence of illegal activity or a violation of Federal law.

Methods used to analyze information include the Special Agent's ability to link events, documents and/or occurrences together in a logical format for the purpose of showing patterns of behavior and relationships associated with an illegal act. The information is used to construct detailed Reports of Investigation (ROI), compile affidavits, search warrants, arrest warrants, and other investigative instruments. All information from public sources, commercial sources or other governmental agencies is acquired to aid the Special Agent in his or her investigation and duty to fully safeguard the Department's interest and administration of Federal funds.

**3.7.** Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

Yes

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

N/A

## Audit Investigations

Testing involves using sample PII in files to validate CMS's ability to detect PII in files. The CMS test environment uses the same security controls as the production environment but is not used to store PII.

## Investigations Application

Testing in the CMS test environment sometimes contains cases with documents that might contain PII. The same provisions that are in place in production are in place in the testing environment. SSNs are removed from individual/index records prior to storage in the test system.

### **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.

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

## Audit Application

As explained in section 1.2, OIG may maintain PII including SSNs provided by auditees when the information itself materially supports conclusions regarding the audit's objectives.

## Investigations Application

SSNs are obtained as a way of confirming the identity of an individual during an investigation. Special Agents obtain SSNs of all individuals who are subjects and victims of investigations to confirm identity. This identity is cross checked with the National Student Loan Data System (NSLDS) and other systems to ensure that the subject of the investigation is in fact the same person who may be involved in fraud, waste, and abuse of Department or other Federal program funds.

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

N/A

### **Audit Application**

Auditors do not ask individuals to supply their social security numbers. Social security numbers may appear in records that the OIG requests from an auditee as part of an audit. Federal student loan records, for example, often contain SSNs. OIG requests alternative identifiers to SSNs for individual records from auditees whenever possible. OIG maintains SSNs when no alternative exists to support OIG findings, conclusions, recommendations, and/or cost recoveries.

### **Investigations Application**

There is no alternative to using SSNs since the NSLDS and the Free Application for Federal Student Aid (FAFSA) systems use the individual SSN to disburse funds. As mentioned above, Special Agents obtain SSNs of all individuals who are subjects and victims in an investigation to confirm identity. This identity is cross checked with NSLDS and other systems to ensure that the subject of the investigation is in fact the same person who may be involved in fraud, waste, and abuse of Department or other Federal program funds.

## **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.

## Audit Application

In response to an audit, Auditors may request records from an auditee that include PII that the auditee has collected or has been provided, and we collect those records from the auditee if the PII is necessary to meet the audit's objective. Notice is provided during the initiation of an audit, but also through the publication of the PIA and the Non-Federal Auditor Referral, Debarment, and Suspension files SORN (18-10-03). During quality control reviews of non-Federal auditors, the OIG may collect records that contain PII about the non-Federal auditor whose work is being reviewed and which may be needed to refer these auditors to State boards of accountancy or to the Department for suspension and debarment. Notice about how this PII is used is covered under SORN 18-10-03.

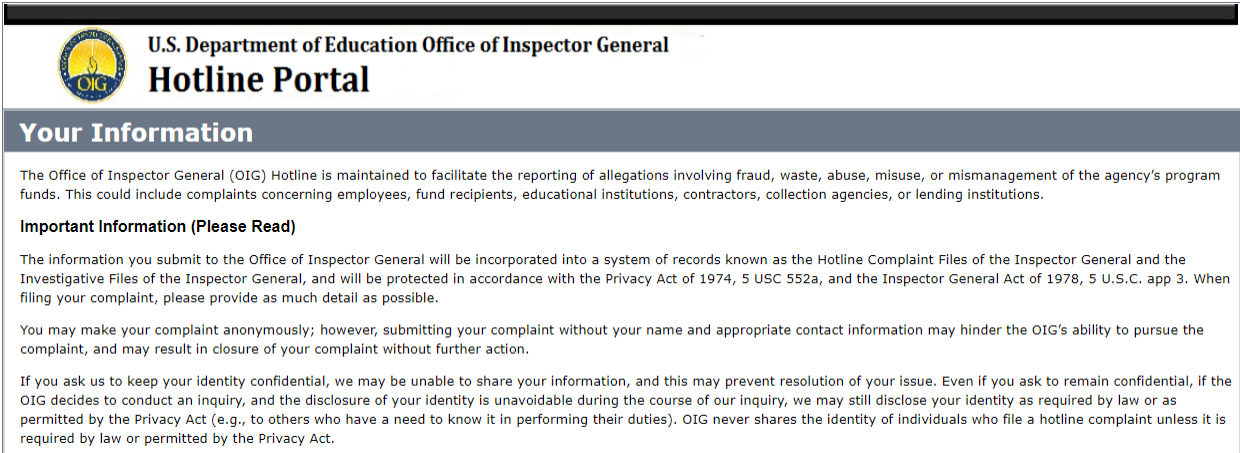
## Investigations Application

The Secretary has, through regulation, exempted the Investigative Files of the Inspector General and the Hotline Complaint Files of the Inspector General from the Privacy Act requirement to give notice to individuals asked to provide information to the Department. (34 C.F.R. § 5b.11(b)(6)).

Notwithstanding this exemption, with respect to hotline complaints, the Department provides information about the Privacy Act to complainants on the online hotline complaint form, <https://oighotlineportal.ed.gov>. If the hotline complainant wishes to remain anonymous, the complaint can be submitted without PII.

- 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



**U.S. Department of Education Office of Inspector General  
Hotline Portal**

**Your Information**

The Office of Inspector General (OIG) Hotline is maintained to facilitate the reporting of allegations involving fraud, waste, abuse, misuse, or mismanagement of the agency's program funds. This could include complaints concerning employees, fund recipients, educational institutions, contractors, collection agencies, or lending institutions.

**Important Information (Please Read)**

The information you submit to the Office of Inspector General will be incorporated into a system of records known as the Hotline Complaint Files of the Inspector General and the Investigative Files of the Inspector General, and will be protected in accordance with the Privacy Act of 1974, 5 USC 552a, and the Inspector General Act of 1978, 5 U.S.C. app 3. When filing your complaint, please provide as much detail as possible.

You may make your complaint anonymously; however, submitting your complaint without your name and appropriate contact information may hinder the OIG's ability to pursue the complaint, and may result in closure of your complaint without further action.

If you ask us to keep your identity confidential, we may be unable to share your information, and this may prevent resolution of your issue. Even if you ask to remain confidential, if the OIG decides to conduct an inquiry, and the disclosure of your identity is unavoidable during the course of our inquiry, we may still disclose your identity as required by law or as permitted by the Privacy Act (e.g., to others who have a need to know it in performing their duties). OIG never shares the identity of individuals who file a hotline complaint unless it is required by law or permitted by the Privacy Act.

- 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?

As noted above, the OIG is not required to give notice to individuals asked to provide information that is stored in the Investigative Files of the Inspector General. Nonetheless, complainants filing hotline complaints are notified via the OIG Hotline Complaint Form that they may file complaints anonymously. Depending on what the complainant is reporting, the OIG may or may not be able to act on an anonymously filed complaint. Additionally, the OIG may employ law enforcement methods to get PII if it is material to an investigation and a person declines to provide it.

**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

The OIG is not required to provide notice, but will update any notices provided as necessary.

## 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?

N/A

### Audit Application

OIG may share files containing PII from the CMS Audit Application with the Department for the purpose of resolving audit findings and recommendations. Files supporting OIG findings and recommendations contained in CMS may be shared with Department components that were the subject of the audit, the Office of General Counsel, and/or the Office of the Chief Financial Officer.

### Investigations Application

PII is shared with the appropriate Department offices whose staff have a need to know the information to perform their duties.

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

N/A

### Audit Application

OIG may share files from the Audit Application containing PII with Department offices that require the records to resolve audit findings and recommendations.

### Investigations Application

Hotline complaints containing PII are routinely shared with the appropriate Department program offices whose staff have a need to know the information to perform their duties. For instance, a complaint submitted by a student to the OIG Hotline that alleges an institution improperly disbursed student aid would be shared on a routine basis with the Federal Student Aid (FSA) office because the OIG does not typically investigate matters involving a single beneficiary. FSA is the appropriate office to timely assist individual students with resolving their concerns. The OIG Hotline is the only unit within the agency responsible for receiving and processing complaints and other inquiries from the public related to fraud,

waste, and abuse of Federal funds in Department programs; however, many of the complaints that the OIG Hotline receives do not rise to the level of a criminal, civil, or administrative investigation. Matters that do not warrant OIG investigations are typically forwarded by OIG Hotline to the appropriate program offices for resolution. PII may also be shared with the Department in written formats, such as through a Management Information Report or other documents, when internal control weaknesses are identified through a criminal, civil, or administrative investigation. If appropriate, the information would be shared with the program office that has oversight responsibility for taking appropriate corrective action to eradicate any reported weaknesses and PII will be made available to those with a need to know it. No PII is made public as part of these reports.

**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.<sup>4</sup>

**Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.**

N/A

---

<sup>4</sup> 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.



## Audit Application

Files containing PII data in the Audit Application may be shared with other Federal OIGs to complete required peer reviews in accordance with generally accepted government auditing standards (GAGAS) issued by the Government Accountability Office (GAO) and Federal requirements developed by the Council of the Inspectors General on Integrity and Efficiency (CIGIE). Staff from other OIGs conducting the peer review must sign a non-disclosure agreement before they are given access.

OIG may also share files containing PII with an auditee for the purpose of resolving audit findings and recommendations.

OIG may also share PII pursuant to the Privacy Act Exemptions, to include routine uses listed in the Privacy Act SORN for the Non-Federal Auditor Referral, Debarment, and Suspension files (18-10-03). PII may be shared with the external entities mentioned in the SORN without the consent of the individual if there is an appropriate routine use and the disclosure is compatible with the purposes for which the record was originally collected.

## Investigations Applications

Name, DOB, SSN, and contact information may be shared with other law enforcement agencies, prosecutors, and other entities identified in the SORNs that cover the system.

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

N/A

## Audit Application

OIG shares files containing PII from the Audit Application with external entities in connection with peer reviews by other OIGs and when required to complete resolution of findings and recommendations with an auditee.

## Investigations Application

Information in the Investigations Application is most frequently shared externally with persons or entities consistent with the Privacy Act exemptions.

In many investigations, the subject violator has committed other violations which may fall under the jurisdiction of other law enforcement agencies. An OIG Special Agent may share the PII of a subject with another law enforcement agency if such sharing is consistent with the Investigative Files of the Inspector General SORN. The OIG is also authorized to share information with persons or external entities specified in 5 USC 552a(b).

**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

Individual disclosures are recorded manually and retained in the system. For example, investigators are trained to record all investigative steps, which may include disclosures of PII, if applicable, in their chronological files, which are files reflecting all of their investigative activity. These records are stored within the system. Any retrieval of these records from the system would be manual retrieval.

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

N/A

## Audit

Records that may contain PII are shared with external entities by extracting information from the Audit Application into an encrypted file that is subsequently shared through a secure Department portal.

## Investigations Application

OIG may transmit records with PII electronically using password-protection, encrypted email, or other Department or law enforcement approved methods for transmitting PII.

**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

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

N/A

No

## **6. Redress**

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

## **Audit Application**

The Non-Federal Auditor Suspension, Referral and Debarment SORN outlines the access procedures for this category of records under 34 CFR 5b.5. Individuals wishing to gain access to a record in this system of records must submit a written request to the system manager.

## **Investigations Application**

Individuals cannot access their own information directly in the system; however, individuals may request a copy of their own records by completing the request form here:

[http://www2.ed.gov/policy/gen/leg/foia/request\\_privacy.html](http://www2.ed.gov/policy/gen/leg/foia/request_privacy.html).

The record access procedures (described in the Department's regulations) are not applicable to criminal investigative files except at the discretion of the Inspector General. See 34 CFR 5b.11(b)(3) and (c)(1); 34 CFR 5b.11(g).

The record access procedures are applicable to non-criminal investigative files under the conditions defined by 34 CFR 5b.11(c) and (f). Under these conditions, the procedures are governed by 34 CFR 5b.5.

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

## **Audit Application**

The procedures for correcting Non-Federal auditor Suspension, Referral, and Debarment records covered under SORN 18-10-03 are contained in 34 CFR 5b.7. These files are a subset of files in the audit application that are retrieved by name or other personal identifier and are subject.

The procedures for correcting training records covered under SORN OPM/Govt-1 (General Personnel Records) are contained in 34 CFR 5b.7.

## **Investigations Application**

The procedure in the Department's regulations for correction or amendment of records is not applicable to criminal and non-criminal investigative files. 34 CFR 5b.11(b)(3) and (c)(1).

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

## Audit Application

The OIG notifies individuals about procedures for correcting their information in the publicly available Non-Federal Referral, Suspension and Debarment SORN and in the General Personnel Records SORN.

## Investigations Application

The record access procedures (described in the Department's regulations) are not applicable to criminal investigative files except at the discretion of the Inspector General. See 34 CFR 5b.11(b)(3) and (c)(1), 34 CFR 5b.11(g)

The record access procedures are applicable to non-criminal investigative files under the conditions described in 34 CFR 5b.11(c) and (f).

The procedures for requesting access are outlined in 34 CFR 5b.5

### 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?

The appropriate NIST 800-53 Rev 4 controls are implemented in the CMS. The system has undergone an assessment of risk and received an authorization to operate, and continuous monitoring is used to ensure continued technical protections. This includes, but is not limited to, two-factor authentication, encryption of data at rest, and access controls based on user

profile. Access to the system can only be achieved from a computer connected to the Department network, and the software and operating system has extensive logging. The infrastructure that hosts the CMS employs firewalls, intrusion detection/prevention systems, anti-virus software, and the system is routinely scanned for vulnerabilities.

Administrative safeguards are also used. For example, all government employees and contractors must possess at least a 5c public trust clearance and an HSPD-12 PIV card prior to being granted access to CMS. To obtain access, an account must be created within the CMS and appropriate profile will be created to grant access to data based on a need-to-know basis and the least allowable privilege needed to perform required duties. The system is FedRAMP SaaS authorized and undergoes a third party (3PAO) annual assessment.

**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 system is FedRAMP SaaS authorized and undergoes a third party (3PAO) annual assessment. OIG receives and reviews monthly deliverables, POA&M list, scan reports, and asset inventory list, to ensure the system is securely operating as intended.

## **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?

### **Audit Application**

Audit supervisors review and approve all files containing PII in CMS in accordance with OIG policies and procedures. When an audit project is ready to be closed, the audit supervisor conducts a final review and prepares the finalization checklist. An audit manager approves the finalization checklist.

## Investigations Application

Investigative supervisors review investigative files on a quarterly basis for accuracy. When a case is ready to be closed, a final review by a supervisor is conducted to ensure information is accurate.

- 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. To mitigate these risks, OIG has implemented security and privacy controls consistent with OIG, Department, and Federal requirements.