U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction:

The Department of the Interior (DOI) requires the DI-4001 Privacy Impact Assessments (PIA) form to be conducted and maintained for all IT systems that collect, maintain, use, or share personally identifiable information (PII), whether the system is new, undergoing significant modification, or already in operation as well as electronic collections under the Paperwork Reduction Act. The PIA is a critical tool for evaluating privacy risks, documenting safeguards, ensuring compliance with the E-Government Act of 2002 (Section 208) and OMB Guidance. This form must be completed electronically and submitted to the Department Privacy Office for review and determination via our Privacy Office Support Request Page. For further guidance, consult the DOI PIA Guide.

System Information

System or Project Name:	OIG General Support System
System or Project Acronym:	OIG-GSS
Date submitted for review:	July 10, 2026
System Operational Status:	Modification

Point of Contact

Name:	Danielle Sanzi
Title:	Privacy Officer
Office:	Office of the Inspector General
Phone:	771-216-1220
E-mail:	oig_privacy@doioig.gov

Section 1: System Overview

1. What triggered this PIA? (Check one)

☐ New System
☐ New Electronic Collection
☒ Significant Modification
☐ Other: Describe below

This PIA is being conducted due to a significant modification to the Office of the Inspector General-General Support System (OIG-GSS). This modification adds the Data Analytics Unit (DAU) Dashboard Portal, a minor application, to this system. The DAU Dashboard Portal sources data from Department of the Interior (DOI) systems, Federal and State agency systems, and publicly available data. A separate PIA has been conducted for the DAU Dashboard application and is published on the DOI Privacy webpage at https://www.doi.gov/privacy.

2. What is the purpose of the system or project?

The mission of the OIG is to provide independent oversight to promote accountability, integrity, economy, efficiency, and effectiveness in the programs, operations, and management of the DOI.

The OIG-GSS is an operational system, composed of network computing hardware and related software in support of network management and monitoring tools, database storage platforms, wireless services, active directory management and monitoring, file system management, security tools, and office automation tools. The OIG-GSS supports OIG employees and the operational day-to-day OIG oversight responsibilities in conducting independent investigations, audits, inspections, and evaluations on programs administered by the DOI. The OIG reports our findings of fraud, waste, abuse, and mismanagement to Department officials, Congress, the U.S. Department of Justice (DOJ), other law enforcement entities, and the public. The Information Technology Division (ITD), under the Office of Management for the DOI OIG maintains the overall OIG-GSS network which hosts seven (7) minor applications that are described below in Section 1, Part 7: AMP, Case Management System (CMS), Coding Operations and Development Environment (CODE), Customer Service Portal (CSP), DAU Dashboard Portals, data/evidence storage application, and audit planning software. These minor applications that reside within OIG's GSS security boundary are covered under this privacy impact assessment (PIA) and a separate PIA was conducted specifically for one application - Data Analytics Program DAU Dashboard Portal - described below.

The key tools and software components of the OIG-GSS include:

- Active Directory management for users and computing devices
- Server farm that hosts file and sharing services, database instances, web services, Commercial off-the-shelf (COTS) applications, and utilities
- Security tools to monitor network and utilization
- System auditing applications to capture privileged and non-privileged user activities on the network
- Office automation suites to enhance workspace productivity
- Automated scanning to detect anomalies on the systems, database, web applications, peripherals and other components
- System virtualization to increase efficiency of the computing and storage capacities
- Network storage and backup for disaster recovery
- Personal computing and mobile devices
- Wireless access points
- Data-at-rest and data-in-transit encryption capabilities
- Virtual collaboration tools.

3. Is the system registered in BisonGRC?

☒ Yes: If applicable What is the project's UII code?
☐ No: Explain why this is not either done or required.

The OIG-GSS is registered under UII Code: 010-000002258 - System Security and Privacy Plan for the Office of the Inspector General-General Support System (OIG-GSS). The system record includes current security categorization, privacy impact assessment status, and supporting documentation for the Authorization and Assessment (A&A) process. The BisonGRC record is reviewed and updated during annual FISMA reporting and whenever significant changes are made to the system's design, functionality, or data types.

4. What legal authorities authorize the collection and use of data in this system or project?

The collection and use of data within the OIG-GSS is authorized under the following authorities:

Inspector General Act of 1978, as amended, 5 U.S.C. §§ 401-424 - Enables OIG to perform its oversight and investigative functions. The Inspector General Act of 1978 authorizes OIG to have access to "all records, reports, audits, reviews, documents, papers, recommendations, or other material" maintained by the DOI. Furthermore, it authorizes the execution of search warrants, seizure of evidence, and search of such property. The OIG-GSS supports the activities of the OIG including investigations, audits, inspections, and evaluations.

Privacy Act of 1974, 5 U.S.C. § 552a - Establishes requirements for the collection, maintenance, and disclosure of records that are retrieved by personal identifiers. OIG-GSS contains records that may be retrieved by the names and contact information of OIG and DOI employees; members of the public; and other Federal, State, local, and Tribal individuals.

5. Does the system or project require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: If yes, list the applicable citations below.
☐ No

The OIG-GSS requires coverage under the Privacy Act because records in most of the minor applications are retrieved by personal identifiers. The following SORNs apply to this system.

INTERIOR/OIG-01, Management Information, 55 FR 14480 (April 18, 1990); modification published 86 FR 50156 (September 7, 2021). Categories of records include OIG employee training and performance awards, audit information, and investigative information. Records are retrieved by name.

INTERIOR/OIG-02, Investigative Records - 88 FR 44827 (July 13, 2023). DOI published regulations at 43 CFR part 2, subpart K to exempt certain records in OIG-02 from some provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1), (k)(3), and (k)(5). Records in this SORN include investigative files including complaints, evidence, reports, correspondence and memoranda generated by OIG during an investigation. Records are retrieved by name or case file number.

INTERIOR/DOI-58, Employee Administrative Records - 64 FR 19384 (April 20, 1999); modifications published at 73 FR 8342 (February 13, 2008) and 86 FR 50156 (September 7, 2021). This SORN includes general administrative records. Records are retrieved by name.

INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) - 72 FR 11040 (March 12, 2007); modification published 86 FR 50156 (September 7, 2021). Active Directory user accounts are covered under this SORN and records are retrieved by name.

OPM/GOVT-1, General Personnel Records, 77 FR 73694 (December 11, 2012); modifications published at 87 FR 5874 (February 2, 2022) and 88 FR 56058 (August 17, 2023). This SORN includes general employee personnel files maintained under Office of Personnel and Management (OPM). Records are retrieved by name.

The DAU Dashboard Portal relies on source-system SORNs and the separate DAU PIA for additional source-system coverage. Because DAU is the significant modification triggering this PIA, the DAU PIA or a DAU SORN/source-system crosswalk should be included in the review package. DAU-derived outputs, extracts, dashboards, reports, and analytical work products must be evaluated based on the recordkeeping context in which they are used, including whether they become audit records, investigative records, management records,

or administrative records covered by the applicable SORN.

DOI SORNs, links to government-wide SORNs, and the DAU PIA, which lists all of the source SORNs can be found on the DOI Privacy website at https://www.doi.gov/privacy.

6. Does this project involve an information collection that requires OMB approval under the Paperwork Reduction Act?

☐ Yes
☒ No

Collection of information is limited to federal employees and PII collected on other individuals is not new data. It is sourced from existing data.

7. List all minor applications or subsystems that are hosted on this system and covered under this PIA.

AMP: AMP is a case management application that provides workflow functionalities, accessible only by OIG employees, across OIG offices, including work scheduling, training, small procurement (typically items/services less than $5,000), on-boarding and off-boarding employees, performance awards, report reviewing, and claims for reimbursement for expenditures on official business. PII includes employee full name, personal email address, personal phone number, home mailing address, and emergency contact**.**

Case Management System (CMS): This is OIG's legacy web-based system used by the Office of Investigations (OI) within the OIG that tracked and maintained all complaints, preliminary inquiries, and investigations that OIG Staff used for case management and program referral capabilities. The system was designed to facilitate criminal, civil, and administrative investigations of fraud, waste, and abuse in programs administered by the DOI. CMS generated statutorily required information and management reports, as well as assisted in the overall management and collection of data required for successful investigations and prosecutions. A new system, Case Management Tracking System (CMTS), that is not hosted by OIG-GSS replaced CMS. CMS is still maintained for historical records and reference purposes. This system contains older investigations that will be dispositioned once all cases are closed and ten years thereafter. PII includes Full name, citizenship, sex, birth date, other names used, place of birth, driver's license, SSN, tribal or other ID number, personal email address, personal telephone number, mailing/home address, race/ethnicity, group affiliation, medical information, and any other PII necessary to conduct criminal, civil, and administrative investigations pursuant to the IG Act of 1978, as amended.

CODE: This minor application, only accessible by authorized OIG employees, allows developers within the OIG's ITD and DAU to write and securely store the underlying source code which supports OIG web applications and PowerBI dashboards. PowerBI dashboards, created and maintained by OIG's DAU allows for the analysis of large data, statistical sampling and modeling, and other techniques. PII includes employee full name, and employee email address.

Customer Service Portal (CSP): This is an OIG enterprise-wide application designed to be accessible only by OIG employees. Inherent in the OIG CSP are the following applications: Correspondence Tracking System (CTS); Employee List; Organizational Chart; and internal customer service helpdesks for Audits, Inspections and Evaluations (AIE); Communications; DAU; Facilities and Operations Services(FOS); Financial and Business

Management System (FBMS) access; Financial Management; Office of General Counsel (OGC); Human Resources; Information Technology (IT); IT Security; and OI Operations. Access to those systems is limited to those employees with appropriate authorization. PII includes employee full name, photo, office assignment, location, and phone numbers, and employee email address.

Data Analytics Unit (DAU): The DAU is an internal dashboard portal for selected end users which provides data and statistical support to the OIG. Data is sourced from DOI systems, other Federal agency's systems, State systems and other publicly available data. The DAU obtains data, conducts data analysis, develops dashboards, and performs statistical tests and procedures in support of audits, investigations, and administrative and management initiatives. The DAU database server's access is limited to authorized individuals only. Overall, DAU provides a secure, governed data platform that can be leveraged by auditors and investigators to promote economy, efficiency, and effectiveness. A separate PIA was conducted specifically for the Data Analytics Program and DAU Dashboard Portal and is posted on DOI's website at https://www.doi.gov/privacy. PII includes name, sex, birth date, marital status, financial information, credit card number, law enforcement data, driver's license, race/ethnicity, SSN, personal phone number, tribal or other ID number, personal email address, employment information, mailing/home address, and travel/purchase/fleet card information.

Data/Evidence Storage Application: This application is a web-based, software for reviewing eData collections, e.g., collection of emails and text messages. It stores evidence data securely and is used by OI to filter, search, review, tag, share, and link annotations to metadata and content of eData. It is managed by OI. ITD performs system administration functions. PII includes full name, citizenship, SSN, sex, date of birth, spouse information, personal email address, home mailing address, home phone number, driver's license, race/ethnicity, and any other PII necessary to conduct criminal, civil, and administrative investigations pursuant to the IG Act of 1978, as amended.

Audit Planning Application: This is a web-based software application designed to control audit planning, fieldwork, collaboration, review, reporting, resolution, follow-up, and program efficiency. Data from this application is accessible over the OIG network through client application connections to the centralized database. This audit planning application is OIG's database for electronic audit, inspection, and quality control review project files. The purpose is to facilitate audit management and assignments of personnel, and document audits and inspections in accordance with generally accepted government auditing standards and other policies. PII includes full name, SSN, sex, date of birth, personal email address, financial information, credit card number, group affiliation, and education information.

Section 2: Data Description and Use

1. What categories of PII and sensitive data types will the system collect, use, or store? Check all that apply.

☒ Name (full, first or last)
☒ Aliases/nickname
☒ Driver's license
☒ Citizenship
☒ Legal Status
☒ Sex
☒ Race or ethnicity
☒ Home telephone number
☒ Personal Email
☒ Mailing or home address
☒ Religious preference
☒ Mother's maiden name
☒ Marital status
☒ Spouse Information
☒ Employment or resume info
☒ Full or Truncated SSN
☒ Physical characteristics
☒ Biometrics or facial recognition
☒ Vehicle information
☒ Passport information
☒ Travel information

☒ Date of birth
☒ Place of birth
☒ Personal cell phone number
☒ Tribal or other ID number
☒ Military records
☒ Child or family information
☒ Emergency contact info
☒ Financial information
☒ Education information
☒ Other: Describe below
☒ Parent's name
☒ Credit card number
☒ Nationality
☒ Disability Information

This system may contain and/or use data collected from law enforcement investigations, DOI and OIG employees, personnel records, and information from other Federal agencies through the DAU. Older closed investigative records are maintained in CMS and current investigative records may be temporarily maintained in the data/evidence storage application in the course of investigating individuals. CMS and the data/evidence storage application may contain images or videos collected from digital recording devices captured by special agents. This data is collected during the course of OIG's law enforcement investigations pursuant to the Inspector General Act of 1978, as amended. In addition, for OIG's AIE team, the audit planning application collects records used for audits, inspections and evaluations and may include information on Federal employees and civilian personnel.

2. What is the source for the PII collected? Check all that apply.

☒ Individual
☒ Federal Agency
☒ Tribal Agency
☒ Local Agency
☒ DOI Records
☒ Third Party Records
☒ State Agency
☒ Other: *Describe Below*

For CMS, PII was previously collected directly from the individual through a written form, filing a complaint on the OIG website, and through interviews over the phone, computer, or in person. PII also came from agency officials and employees, or agency systems or records, such as the Federal Personnel and Payroll System (FPPS).

Information collected by the DAU is collected from other Federal agencies and sites such as government contracting information from General Service Administration's (GSA's) System for Award Management (SAM).

CSP and AMP contain forms filled out by OIG employees to request hardware, software, or other IT or office related equipment as well as telework requests and reimbursement requests for authorized expenses. CSP also contains helpdesk surveys that OIG employees may voluntarily complete.

Information in the data/evidence storage application may also be collected through Department records requests, subpoenas, search warrants, seizure of evidence, and voluntary disclosure. This information is collected from investigative activities authorized by the Inspector General Act of 1978, as Amended.

3. How will the information be collected? Check all that apply.

☒ Paper Format
☒ Email
☒ Face-to-Face Contact
☒ Website
☒ Fax
☒ Telephone Interview
☒ Shared Between Systems: *Describe*
☒ Other: *Describe*

AMP and CSP collect data from individual users of the system. DOI OIG requires multi-factor authentication for network and system access.

Although CMS is OIG OI's legacy investigative records system, it collected information from individuals during interviews; via telephone, text message, and email messages; from cellular carriers or internet service providers; and information obtained through data feeds to other Law Enforcement databases or systems. OIG OI also collected information from complainants via the OIG website. In addition to using multi-factor authentication for main system access, only specifically authorized OIG personnel may access CMS and must input a username and password. The PIA for the current investigative tracking system CMTS can be found here: Case Management Tracking System.

For the DAU, data is collected from external sources manually or using a secure application programming interface (API) connection to the data source. DAU data scientists also have privileged access to the respective data stores. External sources of data include Contractor Performance Assessment Reporting System (CPARS), FPPS, FBMS, Financial Procurement and Data System (FPDS), U.S. Department of the Treasury's Do Not Pay (DNP) Portal, PaymentNet, Amazon Business Prime, or SAM.gov.

Code collects name and email address via the individual employee's use of the application. It is a GitLab-based environment which allows OIG's developers to securely write underlying source code. Only specifically authorized OIG personnel may access this minor application.

The data/evidence storage application is a COTS software for reviewing eData. This eData is collected through other means, such as interviews, complaints, data sharing from other Federal agencies, or collection from DOI records. This minor application enables Special Agents and examiners to review and sort large collections of data. Only specifically authorized OIG personnel may access these minor applications.

The audit planning application collects information for audits, inspections and evaluations from the Department, bureaus and other entities receiving grants or funds from DOI programs. Information may be paper-based or electronic. Data is accessible over the OIG network through client application connections to the centralized database. Only specifically authorized OIG personnel may access this minor application.

4. What is the intended use of the PII collected?

The primary use of the PII in the system is to facilitate the OIG's various responsibilities under the Inspector General Act of 1978, as amended. The OIG is statutorily directed to conduct and supervise investigations relating to programs and operations of the DOI, to promote economy, efficiency, and effectiveness in the administration of such programs and operations, and to prevent and detect fraud, waste, and abuse in such programs and operations. Accordingly, records in this system are used within the DOI and OIG in the course of investigating individuals and entities suspected of misconduct, waste, fraud, and abuse, other illegal or unethical acts and in conducting related criminal prosecutions, civil proceedings, and administrative actions. These records are also used to fulfill reporting requirements, to maintain records related to the OIG's activities, and to prepare and issue reports to Congress, the DOI and its components, the Department of Justice, the public and other entities as appropriate within the mission of the OIG.

Additionally, PII is obtained to conduct, supervise, and coordinate audits relating to Department programs and operations as required by the IG Act. Our audit objectives may require that we examine how the Department

and recipients disburse and expend federal funds. This may require the use of PII, such as a charge card number and other PII in audits involving the integrated charge card program.
PII collected from OIG employees accessing the system and its minor applications is for monitoring and auditing purposes and for tracking helpdesk tickets and individual employee requests related to day-to-day operations.

5. How does this project limit the collection and use of PII to only what is necessary?

As this system supports the OIG's various responsibilities under the Inspector General Act of 1978, as amended, the OIG is statutorily directed to conduct and supervise investigations relating to programs and operations of the DOI, and to conduct, supervise, and coordinate audits relating to such programs and operations. The collection of PII is necessary to carry out that mission, but the OIG has controls in place to protect that information.

For AMP, CODE, and CSP only non-sensitive data such as employee name and home phone number is collected. The system does not allow additional fields for collection of sensitive PII.

For CMS and the data/evidence storage application, law enforcement sensitive data that is collected is necessary to carry out the OIG mission. However, access to this information is limited to authorized personnel with proper credentials. DOI OIG requires two-factor authentication for network and system access which is based on least-privilege-access and role-based access controls. Access control lists are created and segmented by OIG offices and users cannot view information for other offices or users unless specifically authorized.

For the DAU, data from multiple sources is collected daily for use in statistical analysis. The DAU sources their data from targeted sites for particular purposes. The DAU may collect more PII than is necessary due to the nature of the system and purpose, as it collects many datasets on a daily basis from multiple sources with PII. Access is limited to authorized DAU personnel.

For the audit planning application, only information that is necessary to carry out the audits, inspections, and evaluations functions is collected. This application collects data from targeted areas within the department for particular purposes and access is limited to authorized AIE personnel.

Section 3: Data Sharing and Individual Rights

1. With whom will the PII be shared, both within DOI and outside DOI? Check all that apply.

☒ **Within the Bureau/Office:** Describe how the data will be used below.
☒ **Tribal, State or Local Agencies:** Describe how the data will be used below.
☒ **Other Bureaus/Offices:** Describe how the data will be used below.
☒ **Contractor:** Describe how the data will be used below.
☒ **Other Federal Agencies:** Describe the federal agency and how the data will be used
☒ **Other Third-Party Sources:** Describe how the data will be used below.

Within the Office:

- For AMP, PII may be shared within the OIG for workflow management and operational support such as

work scheduling, employee onboarding/offboarding, small procurement activities, performance awards, storing/viewing employee agreements or records, and report generation.

- For CODE, PII is not shared.
- For CSP, PII may be shared with each helpdesk to identify individuals such as submitters of helpdesk requests and employees requesting IT related equipment.
- For CMS, PII may be shared within the DOI OIG as part of the investigative or report development process. Access to information is restricted to authorized personnel only.
- For DAU, PII may be shared with OIG personnel in OI, AIE, OGC, or ITD to facilitate the OIG's various responsibilities under the IG Act.
- For the data/evidence storage application, PII may be shared with authorized users within DOI OIG as part of the investigative process. Access to this system itself is strictly limited within the OIG to authorized individuals only.
- For the audit planning application, PII may be shared within the AIE team, OI OGC, or other authorized OIG personnel.

With Tribal, State or Local Agencies:

PII may be shared with Tribal, State and local law enforcement or prosecutive agencies only to the extent necessary to carry out OIG investigations. In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information may be disclosed outside OIG as a routine use pursuant to 5 U.S.C. 552a(b)(3), published in OIG's system of records notices. Any transmission to outside offices is done with encryption, use of password protected documents, or use of OIG's Secure File and Collaboration Portal (OSFCP) which is a separate OIG system with its own PIA located on DOI's website referenced above.

With Other Bureaus/Offices:

PII from this system may be shared with the Office of the Secretary (OS)/other bureaus only to the extent necessary to carry out OIG investigations, audits, evaluations and inspections as well as reporting requirements pursuant to the Inspector General Act.

It is possible that OIG may share PII with OS/other bureaus through shared infrastructure hosted by the DOI. Non-OIG employees do not have access to the OIG-GSS and its minor applications. If there is any business need to share PII residing on OIG's systems (e.g., procurement, payroll, etc.) staff will utilize the Department's systems such as FPPS, O365, SharePoint, Teams, etc., which are not within scope of this PIA and have been evaluated under separate DOI PIAs.

With Contractors:

OIG has contractors who are authorized to perform system development support for minor applications such as AMP and CMS. PII may be shared for the purposes of trouble shooting or technical assistant to the applications.

With Other Federal Agencies:

PII may be shared with the U.S. Attorney's Office or other Federal agencies that are part of an OIG or joint investigation to the extent necessary to carry out OIG investigations or prosecutorial functions. In addition to

those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information may be disclosed outside OIG as a routine use pursuant to 5 U.S.C. 552a(b)(3), published in OIG's system of records notices. Any transmission to outside offices is done with encryption, use of password protected documents, or use of OIG's Secure File and Collaboration Portal (OSFCP) which is a separate OIG system with its own PIA located on DOI's website referenced above.

With Other Third-Party Sources:

PII may be shared with any Third-Party source to the extent necessary to carry out OIG investigations. In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information may be disclosed outside OIG as a routine use pursuant to 5 U.S.C. 552a(b)(3), published in OIG's system of records notices.

All sharing is consistent with the purposes outlined in INTERIOR/OIG-1, Management Information, 55 FR 14480 (April 18, 1990); modification published 86 FR 50156 (September 7, 2021) and INTERIOR/OIG-02, Investigative Records, 88 FR 44827 (July 13, 2023), which may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn. DOI published regulations at 43 CFR part 2, subpart K to exempt certain records in OIG-02 from some provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k).

2. Does this system have an MOU/MOA/ISA with other Federal Agencies or State/Local/Tribal Agencies with which it shares information?

☒ Yes
☐ No

There is an Interconnection Security Agreement with the U.S. Department of Treasury (Treasury) Do Not Pay (DNP) System. The purpose of this agreement is to access Treasury's DNP system for official purposes related to identifying, preventing, and recovering improper payments. This agreement also permits sharing OIG data with Treasury for comparison with other agencies' source data. PII may include names and contact information. The OIG retains full control over its records. The OIG ensures compliance with data governance, security, and access control policies for the use of this system.

3. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII? If not, what steps are in place to ensure individuals are aware of how their information is being used?

☐ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*
☒ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

Due to the purpose and nature of the system, and to help facilitate the OIG's various responsibilities under the Inspector General Act of 1978, as amended, generally individuals will not have the opportunity to consent to the collection or use of their information. Special Agents may use information contained in CMTS and CMS for information sharing. CMS, OIG's legacy application for maintaining investigative files, does not collect new information, except for authorized OIG employees accessing the application. Those activities as well as the activities logging onto the other minor applications in this system, are monitored and employees must consent

to the use of their PII in order to enter the applications.

Individual members of the public do not access or provide direct information into this system and its minor applications. For employees who use DOI email, DOI OIG owned electronic assets, and audio and visual recordings, and for individuals who enter on Federal properties, there is no reasonable expectation of privacy. Individuals who use the DOI network must acknowledge a warning banner that advises them that their information is collected and activity monitored. Data is used only as described in this PIA and the applicable SORNs.

4. How does the project provide notice to individuals prior to the collection of information? Check all that apply.

☐ Privacy Act Statement:
☒ Privacy Notice:
☒ Other: *Describe Below*
☐ None: *Example - law enforcement cases.*

Notice is provided through the publication of this PIA and the publication of the related SORNs referenced above which may be viewed on the DOI SORN website at https://www.doi.gov/privacy/os-notices. For specific law enforcement investigations, notice is not provided at the time of collection to protect the integrity of the investigation, as authorized under the Privacy Act's law enforcement exemption provisions.

Individuals who use the DOI network and access all minor applications in this system receive a warning banner that advises them that their information is collected, and activity monitored and that they have no expectation of privacy. Some DOI controlled areas may have signs posted that inform individuals of surveillance activities, but in many cases, notice may not be provided, or consent obtained for audio or images captured during law enforcement activities.

5. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

AMP data is retrieved by employee name or by the request Folder ID# which is generated by the system and assigned to each request. For instance, a report could be run to show all work schedules submitted by a specific employee. Or a report could be run to show all work schedules submitted in a specific year.

CMS allows records to be queried by an individual's name, case number, or document title.

Users of CODE do not retrieve information by personal identifier.

CSP data is retrieved by a system generated request reference number. Only OIG authorized employees or administrators can access request data. Employees can also retrieve employee information by entering in a name or work location in the employee directory.

For DAU, depending on the dashboard illustration and the data types involved, data can be retrieved by filtering or searching by name. However, users will only be able to search and view content/data from dashboards in which they have been explicitly granted access.

For the data/evidence storage application, data is retrieved by manually entering keywords relevant to the

nature of the case. Identifiers may include subject names, addresses, phone numbers, email addresses, SSN (rarely, on occasion), or any other identifier contained within the system. Data can also be automatically filtered by date/time, file type, or other file metadata non-specific to an individual.

The audit planning application data is generally retrieved based upon assignment number and project name. Key word searches can be used within a project. Data is not retrieved by personal identifier.

6. Will reports be produced on individuals, whose PII is contained in this system? If yes, who has access and what is the purpose of these reports?

☒ Yes: Describe the use of these reports and who will have access to them.
☐ No

Both CMS and the data/evidence storage application applications have the capability to produce case-based reports involving information on individuals (subjects) of an investigation. The report is used as supporting documentation for an investigation. Such reports may be shared within OIG, with other DOI bureaus, with other Federal agencies outside of DOI (e.g., DOJ, FBI, etc.), or with tribal, state or local law enforcement agencies, consistent with the routine uses published in INTERIOR/OIG-01 Management Information and INTERIOR/OIG-02 Investigative Records SORNs referenced above. These applications are only accessible to OI personnel and other authorized OIG users.

In addition to case-based reports, the OIG-GSS and most minor applications have auditing capabilities. Audit log reports consist of user-based activity with session-related actions. Prior to logging into any IT system or application, OIG users must acknowledge and give consent to electronic monitoring which produces audit logs. Monitored activities include login attempts (both successful and unsuccessful); password changes; artifacts accessed; and folders/files created, modified, or deleted. Users are uniquely identified by username and each event is time-stamped. Audit logs or reports are used for monitoring purposes in support of FISMA requirements as well as incident management processes. Audit logs are only accessible by OIG ITD administrators or the application administrator.

Any DAU dashboard can be exported as a report in the following formats: .xlsx, .pptx, and .pdf. The purpose of these dashboard reports is to provide ad hoc support for individual audits, investigations, and OIG projects as well as ongoing data analysis through DAU's portals. On screen, these reports are accessible to OIG personnel assigned to a specific group such as AIE, HR, ITD, or OI, but it may be shared internally with OIG senior leadership. On occasion, there could be limited circumstances where a report may be shared outside OIG as a routine use published in INTERIOR/OIG-01 Management Information and INTERIOR/OIG-02 Investigative Records SORNs referenced above.

7. How will data collected from sources other than DOI records be verified for accuracy?

AMP and CSP data are not collected from other sources outside of DOI. CMS data is verified for accuracy by the individual collecting the data per OIG Office of Investigations policy and procedures. Supervisors will also review for accuracy. The data/evidence storage application data is collected by and received from the OIG OI Computer Crimes Unit (CCU). The hashing process is an algorithm that provides a "digital fingerprint" that can uniquely identify a particular set of data. While the documents themselves are authenticated through this hashing process, the contents and implications of those documents will be utilized by OIG agents and analysts to

independently corroborate or verify the accuracy of data collected per OIG policy and procedures. Supervisors will also review data for accuracy. The audit planning application data will be verified for accuracy as part of the audit process by auditors and supervisors. The exact methods will depend upon the nature of the data and the objectives of the audit.

DAU collects information from various systems; therefore, each data owner is responsible for the accuracy of the data that is processed by the DAU. All work products from DAU require a full quality assurance check by another member of the DAU for accuracy. Additionally, all DAU dashboards and data portals undergo quarterly reviews by rotating members of the DAU to ensure accuracy, including the requirement to trace back to source documentation. These practices are documented in a formal Quality Assurance Standard Operating Procedure maintained by the DAU as part of a host of DAU policies and procedures.

Section 4: Data Management and Retention

1. What is the retention period for the data and under what records schedule?

Records from the following systems are retained and dispositioned in accordance with the NARA-approved DOI retention schedules as listed below:

AMP records

Schedule Title: General Administration Files
Schedule #: DRS 1.1.0001
Disposition Authority #: DAA-0048-2013-0001-0001
Disposition: Temporary. Cut off at the end of the fiscal year in which the record is created. Destroy 3 years after cut-off.

Schedule Title: Routine Procurement Files
Schedule #: DRS 1.3.0011
Disposition Authority #: DAA-0048-2013-0001-0011
Disposition: Temporary. Cut off on final payment. Destroy 7 years after cut-off.

Schedule Title: Employee Training Files
Schedule #: DRS 1.2.0005
Disposition Authority #: DAA-0048-2013-0001-0005
Disposition: Temporary. Cut off when superseded or obsolete. Destroy 7 years after cut-off.

Schedule Title: Agency Award Files
Schedule #: DRS 1.2.0004
Disposition Authority #: DAA-0048-2013-0001-0004
Disposition: Temporary. Cut off on approval or disapproval of award. Destroy 3 years after cut-off.

CSP records

Schedule Title: Tracking and Control files

Schedule #: DRS 1.1.0003
Disposition Authority #: DAA-0048-2013-0001-0003
Disposition: Temporary. Cut off after the date of the latest entry. Destroy when no longer needed.

Data/evidence storage application and CMS records

Schedule Title: Historically Significant Investigative Records
Schedule #: 2802.1
Disposition Authority #: N1-048-10-03
Disposition: Permanent. Cut off at end of fiscal year in which the investigation is concluded. Transfer to NARA 25 years after cutoff.

Schedule Title: All Other Investigative Records
Schedule #: 2802.2
Disposition Authority #: N1-048-10-03
Disposition: Temporary. Cut off at end of fiscal year in which the investigation is concluded. Destroy 10 years after cutoff.

Audit planning application records

Schedule Title: Audit Files
Schedule #: 1210.3
Disposition Authority #: N1-048-08-22
Disposition: Temporary. Cut off when the final audit report is made. Destroy 7 years after cutoff.

Federal Records identified with a temporary retention which have met their retention date and are not subject to a preservation hold are eligible for disposal and may be disposed of in accordance with 44 USC 3308.

The records retention schedule for DAU records can be found in the DAU PIA located on the DOI Privacy website https://edit.doi.gov/privacy/pia.

2. What measures are in place to validate the accuracy and completeness of data received from external sources?

For AMP and the audit planning application, data completeness is evaluated as part of the audit process. The exact methods depend on the nature of the data and the objectives of the audit. Otherwise, data is validated through the review process. CSP and CMS applications include input validation checks to ensure that mandatory/required fields are filled out before OIG employees successfully click submit button. In addition, individuals and supervisors verify the completeness of data collected. Supervisors review data for completeness for the Data/evidence storage application.

DAU collects information from various systems; therefore, each data owner is responsible for the completeness of the data that is processed by the DAU. OIG personnel within HR, AIE, and OI will verify the completeness of data collected per OIG policy and procedures. Supervisors will also review data for completeness. Additionally, all DAU dashboards and data portals undergo quarterly reviews by rotating members of the DAU to ensure completeness, including the requirement to trace back to source documentation. These practices are

documented in a formal Quality Assurance Standard Operating Procedure maintained by the DAU as part of a host of DAU policies and procedures.

3. Does the project include logging capabilities to record and monitor access to PII?

☒ Yes
☐ No

The OIG-GSS and most minor applications have auditing/logging capabilities. Audit logs consist of user-based activity with session-related actions. Prior to logging into any IT system or application, OIG users must acknowledge and give consent to electronic monitoring which produces audit logs. Monitored activity includes login attempts (both successful and unsuccessful); password changes; artifacts accessed; and folders/files created, modified, or deleted. Users are uniquely identified by username and each event is time-stamped. Audit logs are only accessible by OIG ITD administrators or the application administrator and are reviewed on a weekly basis. System user records are managed in accordance with DAA-0048- 2013-0001-0013, System Maintenance and Use. These records are temporary and will be destroyed no later than 3 years after cutoff when the records are no longer needed for administrative, legal, audit, or other operational purposes.

Section 5. Privacy Risks and Mitigation Strategies

1. What privacy risks are associated with the collection, use, retention, and disclosure of PII, and how are they mitigated at each stage of the information lifecycle?

The OIG-GSS presents several privacy risks due to the volume and sensitivity of PII captured pursuant to the OIG mission and maintained in the system. The following summarizes how privacy risks are managed across each stage of the information lifecycle: collection, use, retention, processing, disclosure, and destruction.

Only authorized personnel with proper credentials can access the data in the system. DOI OIG requires multi-factor authentication for network and system access. Access control lists were created and segmented by OIG office. Users cannot view information for other users unless specifically authorized. Furthermore, OI, AIE, and ITD implement and enforce policies and procedures concerning the protection and disclosure of PII.

Integrated Windows Authentication is used to control access to the systems and is further enhanced with specific AD security groups. Connections between the client application and the server are encrypted. Audit logs are maintained and reviewed at both the database server level and the application level by the system administrators.

Collection Risks: The system and its applications may collect more information than is necessary, particularly during the collection of data for audits and investigations. To mitigate this, only data that supports and is pertinent to the OIG mission is collected and maintained. There is also a risk that individuals may not have adequate notice about the collection and use of their PII. The type and category of data collected is accurately stated in this PIA and in the published SORNs described in Section 1, Question G above. However, the Privacy Act exemptions claimed under 5 U.S.C. 552a(k) limit the applicability of certain notice and access rights to protect law enforcement investigations, which may preclude direct notification in some cases.

Use Risks: There is a risk of unauthorized access and usage of PII while using the system and its minor applications. This is mitigated by the nature of the system. The OIG-GSS and its minor applications are internal, non-public facing information systems. Only DOI OIG employees have access to data on a "need-to-know" basis, and by role-based permissions. Processing occurs only on OIG-furnished laptops with BitLocker encryption and use of PIV and pin for authentication. Authorized personnel using these systems are required to follow operational security protocols and receive specialized training in data handling.

Retention Risks: There is a risk of retaining information longer than necessary and making outdated data available. This is mitigated by the OIG's strict adherence to maintain all records with PII in accordance with NARA-approved DOI retention schedules.

Disclosure Risks: There is a risk of unauthorized sharing or loss of data integrity and confidentiality, which could compromise investigations or individual privacy. This is mitigated by using BitLocker encryption and PIV authentication when accessing GFEs and each user has role-based access, rights, and permissions. Sharing is limited to specific roles within the OIG and governed by the routine uses outlined in the INTERIOR OIG-01/OIG-02 SORNs. All disclosures are logged, and audit trails are maintained to detect and deter unauthorized activity.

Disclosure risks also are present when sharing data with other law enforcement organizations or prosecutorial agencies. If information is shared outside of DOI OIG, it is done through a secure sharing platform called Box, a FedRAMP authorized cloud service provider. There is a separate PIA for Box and it is not hosted by OIG-GSS. Supervisor approval is required when sharing information outside of OIG. The authorized sharing of information in support of law enforcement activities is described in the routine uses published in the OIG-02 SORN.

2. Does the system generate new data or inferences through aggregation or analytics that may influence decisions or individual records? If so, how are those data verified, used, and protected?

☒ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*
☐ No

For the Data/evidence storage application, the system is capable of producing communication network diagrams, timelines, and charts from statistical information within the data set. The Data/evidence storage application supports OIG investigations that may involve data that identifies individuals and their related information or associations, which may be obtained from multiple sources instead of directly from the individual. There is a risk that data from different sources may be aggregated and may provide more information about an individual than is necessary. Data within the application is internal to OIG and only authorized users have access to the system. Data from this application is not shared outside of the OIG.

For the DAU and audit planning application, data aggregation may yield new data elements discovered during an investigation or audit. The risk involving data aggregation has been mitigated since data is only accessible by OIG personnel with a need-to-know, supervisory approval, and membership to a specific email distribution group or security group.

3. Will the new data be placed in the individual's record?

☒ Yes: *Provide explanation below*
☐ No

For the DAU and Data/evidence storage applications, results of analysis or reports may be included in the individual's (subject's) record as necessary and required for OIG investigations. For AMP, new data for employees may include items such as awards and updated work schedules and telework agreement records. Only authorized OIG employees may access DAU and the Data/evidence storage application and OIG employees may only access their own individual information on AMP (with the exception of Human Resourses personnel).

4. Can the system make determinations about individuals that would not be possible without the new data?

☒ Yes: *Provide explanation below*
☐ No

The DAU and Data-evidence storage applications support OIG investigative activities, which may include gathering of evidence or generating reports during investigations that result in determinations about individuals. Reports of investigations may be shared internally and externally as authorized and necessary to meet criminal, civil and administrative law enforcement requirements, consistent with the routine uses in OIG's SORN, OIG-02, Investigative Records, which may be viewed on the DOI SORN website at https://www.doi.gov/privacy/doi-notices

5. How will the new data be verified for relevance and accuracy? Enter N/A if new data is not derived or created.

The DAU dashboards cannot check for accuracy of the information. The data owner for each data source (e.g., web application, system, etc.) is responsible for the relevance and corroboration of any data identified as relevant to any employment record, financial audit, or law enforcement investigation. All DAU dashboards and data portals undergo quarterly reviews by rotating members of the DAU to ensure accuracy, including the requirement to trace back to source documentation.

For the Data/evidence storage application, any new information that is extracted and used in an investigation is manually uploaded into investigative systems and is reviewed and authenticated by OI staff including special agents. Data is validated through investigative means.

The audit planning application data is reviewed and verified based on the information on file.

Section 6: Automated Decision-Making and AI Risk Management

1. Does the system use AI, machine learning, or have a non-operational AI Component?

☒ Yes
☐ No, *Proceed to Section 7.*

2. How are models validated for fairness, accuracy, and transparency?

DAU analytical methods, dashboards, and work products are validated through documented quality assurance procedures, source-data traceability, peer review, and supervisory review. Data owners remain responsible for

the accuracy and completeness of source data. DAU personnel validate outputs by tracing results back to source documentation, reviewing dashboard logic, and conducting periodic reviews of dashboards and data portals. Outputs are used as analytical support for authorized OIG personnel and are not used as the sole basis for decisions about individuals.

Where statistical models, anomaly detection, or machine learning techniques are used, the methodology, source data, assumptions, limitations, and validation steps should be documented in the DAU PIA, DAU standard operating procedures, audit workpapers, investigative files, or other applicable project documentation. This documentation supports transparency by allowing authorized reviewers to understand how outputs were generated, what data sources were used, and what limitations apply.

3. Are individuals notified of AI-based decisions that affect them?

☐ Yes
☒ No

The system does not make AI-based decisions that directly affect individuals. DAU analytics, dashboards, anomaly detection, and related outputs are used to support human review by authorized OIG personnel. Any audit, investigative, administrative, civil, or criminal determination is made by OIG personnel or other authorized officials based on the full record, applicable law, policy, corroboration, and human judgment, not solely on an AI or machine-learning output.

Notice is provided through this PIA, applicable SORNs, system warning banners, and other notices where applicable. For law-enforcement or investigative matters, direct notice may be limited when notice would compromise an investigation or where Privacy Act exemptions apply.

4. Are safeguards in place to prevent bias or unintended consequences?

☒ Yes
☐ No

Safeguards are in place to reduce the risk of bias, erroneous conclusions, or unintended consequences from analytics or data aggregation. DAU outputs are subject to human review, source-data traceability, peer review, quality assurance checks, and supervisory review before they are relied upon. Data owners remain responsible for source-data accuracy and completeness. OIG personnel are responsible for corroborating analytical outputs before using them in an audit, investigation, report, referral, or other official action.

Access to DAU dashboards and related outputs is limited to authorized OIG personnel with a need to know. Outputs are protected through role-based access controls, audit logging, security groups, and applicable OIG policies and procedures. DAU analytics do not independently make determinations, assign legal responsibility, initiate enforcement action, or replace human review.

5. Are models periodically reviewed or retrained to ensure ongoing reliability?

☒ Yes
☐ No

DAU dashboards, analytical methods, and data portals are periodically reviewed to confirm accuracy, completeness, and continued reliability. DAU conducts quality assurance reviews, including reviews that trace outputs back to source documentation. When dashboards, data sources, analytical logic, or use cases change, DAU personnel review and update the applicable methodology, documentation, and controls.

To the extent the DAU uses statistical models, anomaly detection, or machine-learning techniques, those models or methods are reviewed as part of DAU quality assurance, dashboard maintenance, and project-specific review. The system does not use federated learning or train models across decentralized systems. If a future DAU capability involves model retraining using PII, Privacy Act records, or source-system data, additional privacy review, AI governance review, and documentation will be required before implementation.

6. Is federated learning used for privacy-preserving model training?

☐ Yes
☒ No

OIG-GSS and DAU do not use federated learning for privacy-preserving model training. DAU analysis occurs within authorized OIG-controlled environments using approved data sources and access controls. The system does not train models across decentralized devices or servers while keeping source data in place. Privacy risk is mitigated through data access restrictions, role-based permissions, source-data controls, quality assurance review, audit logging, and human review rather than federated learning.

Section 7: Security and Access Controls

1. Who will have access to project data and how is access determined, authorized, and restricted? Check all that apply and respond in the space below.

☒ Users
☒ Contractors
☒ Developers
☒ System Administrator
☐ Other: *Describe below*

Each application is internally facing, so users must first provide multifactor authentication (PIV card and a PIN) in order to access these applications. Users also must accept a warning banner that informs them they are entering a government system and any activity will be monitored. Access is based on specific role and only authorized OIG personnel have access to the particular application. Access is approved by the System Owner and Information owners of the minor applications.

Developers have a separate administrative account to obtain privileged access to the applications and their data. Contractors who are authorized to perform system development support for minor applications such as AMP or CMS may have access to PII for the purposes of troubleshooting or providing technical assistance to the OIG.

2. What data protection policies apply to cloud-based PII storage?

There is no cloud-based PII storage in this system.

3. How does the system monitor and detect unauthorized access, use, or exfiltration of PII?

As with any Federal information system, users are informed upon login that there is no expectation of privacy and that their user session will be monitored for inappropriate use. Users are required to acknowledge and comply with DOI Rules of Behavior for use of computer systems.

OIG ITD deploys monitoring devices strategically within the enterprise to collect organization-defined essential information using a variety of security tools. User activity is logged at both the database and application level. At the database level the User ID, IP address, time, and date of successful and unsuccessful access attempts are logged. At the application level, the username, date, time and specific project accessed is logged. The specific files accessed within a project are not logged unless a change is made. Monitoring of this system will identify who edited a record, but not the specific changes that were made.

4. Does the project include any monitoring of user activity or tracking of individuals? If so, what controls ensure the appropriate use of this capability by authorized personnel?

☒ Yes: describe what controls ensure authorized and appropriate use of this capability.
☐ No

User activity is monitored and reviewed through audit logs at both the database and application level. At the database level the User ID, IP address, time, and date of successful and unsuccessful access attempts are logged. At the application level, the username, date, time and specific project accessed is logged. The specific files accessed within a project are not logged unless a change is made. Monitoring of this system will identify who edited a record, but not the specific changes that were made. Data collected may include physical attributes of an individual (including photos), home and work addresses, phone numbers, and personal email addresses.

As with any Federal information system, users are informed upon login that there is no expectation of privacy and that their user session will be monitored for inappropriate use. The OIG-GSS follows NIST SP 800-53 Rev 5 and DOI Policies and users are required to acknowledge and comply with the Rules of Behavior agreement. Data collected for user activity is enforced through least privilege and requires employee supervisor and system owner approval to gain access to those logs. Privileged users are required to acknowledge and sign a Privileged User Access Agreement (PUAA) annually, which includes a more stringent Rules of Behavior agreement. In addition, all privileged user activity is based on job responsibilities and is audited and reviewed.

5. Will contractors be involved in the following project activities? Check all that apply.

☒ Design
☒ Development
☒ Maintenance

Contractors are involved with AMP and CMS and are subject to the same requirements and standards and rules of behavior for accessing government systems as federal employees. Contractors must take Information Management and Technology (IMT) Awareness Training and role-based privacy and security training.

Developers have a separate administrative account to obtain privileged access to the applications and their data.

Contractors who are authorized to perform system development support for minor applications for AMP or CMS may have access to PII for the purposes of troubleshooting or providing technical assistance to the OIG.

6. What physical, technical, and administrative controls are implemented to protect PII? Check all that apply.

Physical Controls

☒ Security Guards
☒ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☒ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Lock
☐ Other: *Describe Below*

This system uses multiple layers of physical controls to protect PII. One or more of DOI OIG buildings are monitored by security guards. Access to OIG facilities are guarded by key guards, identification badges, and locked file cabinets. All DOI OIG spaces are located within a secure facility and monitored by closed circuit television.

Technical Controls

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Other: *Describe Below*
☒ Intrusion Detection Systems (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☐ Biometrics

Certain technical controls such as firewall, user identification, IDS, VPN, and PIV are implemented by OIG. Only personnel who have monitoring authority can access the logs and security tools to ensure non-privileged/unauthorized personnel cannot gain such access without appropriate approval.

Administrative Controls

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☐ Other: *Describe Below*
☒ Methods to Ensure Only Authorized Personnel Have Access
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Records and Privacy Training
☒ Regular Monitoring of Users' Security Practices

This system employs multiple administrative controls to protect PII.

- Annual DOI privacy and security training for all users
- Periodic security audits and vulnerability scans to assess control effectiveness
- DOI Rules of Behavior acknowledgment required before account activation.
- Regular access reviews to ensure privileges remain appropriate for user roles.
- Formal incident response procedures that require reporting suspected privacy breaches to the DOI-CIRC

and Privacy Officer within one hour.

7. What processes are in place for individuals to file a Privacy Act complaint relating to the project?

This system is an internal system established to support the investigative and audit activities of the OIG. An OIG employee may request to update or change their personal information via the OIG Helpdesks. Due to the purpose and nature of the system, to help facilitate the OIG's various responsibilities under the Inspector General Act of 1978, as amended, generally individuals outside of the OIG will not be able to amend a record that contains their PII. Certain records contained in INTERIOR/OIG-02, Investigative Records, are exempt from provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1), (k)(3), and (k)(5) because of criminal, civil, and administrative law enforcement requirements. For those records that are not exempt, individuals can submit a Privacy Act complaint to Privacy Office, Office of Inspector General, U.S. Department of the Interior, 1849 C Street NW, Mail Stop 4428, Washington, D.C. 20240, or email address at oig_privacy@doioig.gov.

8. What processes are in place for individuals to access their information?

Certain records are exempt from provisions of the Privacy Act as stated above. For records that are not exempt, Individuals can request access to their records, by filing a Privacy Act or FOIA request through FOIA.gov. DOI OIG is no longer receiving Privacy Act requests via email. Requests may also be made in writing via U.S. Postal Mail to Privacy Office, Office of Inspector General, U.S. Department of the Interior, 1849 C Street NW, Mail Stop 4428, Washington, D.C. 20240. An individual requesting records about him/herself must verify his/her identity before OIG will process the request. A certificate of identity form must be completed and can be found on FOIA.gov.

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

Due to the purpose and nature of the system, to help facilitate the OIG's various responsibilities under the Inspector General Act of 1978, as amended, generally individuals outside of the OIG will not be able to amend a record that contains their PII. Certain records contained in INTERIOR/OIG-02, Investigative Records, are exempt from provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1), (k)(3), and (k)(5) because of criminal, civil, and administrative law enforcement requirements. An OIG employee may request to update or change their personal information via the OIG Helpdesks.

10. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The System Owner is responsible for assuring proper use of data and is operated in compliance with NIST Standards. The Information System Security Manager and the Information System Security Officer monitor technical safeguards, review suspicious activity and are responsible for reporting any loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information to the DOI-CIRC, DOI's incident report portal, as soon as possible. The Associate Privacy Officer (APO) is also informed and must ensure that any Privacy breach is reported to the DOI-CIRC. All authorized users are responsible for reporting any compromising, suspected or confirmed breach of data to ITD, the APO or their supervisor.

Section 8: Incident Response and Review

1. In the event of a privacy breach, what steps will be taken to mitigate harm, notify affected individuals, and report to oversight agencies?

In the event of a Privacy Breach, immediate steps will be taken to contain the breach, e.g., recalling an email containing PII. Any suspected or actual Privacy breach will be reported to the DOI-CIRC as soon as possible following a breach. The DOI-CIRC is responsible for reporting any Privacy Breach to the Cybersecurity & Infrastructure Security Agency (CISA). The APO, along with the Breach Response Team, if applicable, investigates any breach and determines the scope of the breach, takes remedial action, completes a risk assessment, and commences notification to affected individuals, if applicable. DOI OIG follows breach response protocols according to OMB M-17-12 Safeguarding Against and Responding to the Breach of Personally Identifiable Information and DOI's Breach Response Plan.

2. How often will this PIA be reviewed and updated to reflect changes in privacy risks or system operations?

This PIA will be reviewed at a minimum every 3 years. This PIA is a living document and will be updated whenever major changes occur to the system's technology, data, or operations that could affect privacy risks, or when there is a change in information handling, collection, use or purpose within the system. If no significant changes are made to this system, it is also reviewed annually through the Privacy Threshold Analysis review.