U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: OIG General Support System (OIG-GSS)
Bureau/Office: Office of Inspector General
Date: 6/17/2021
Point of Contact:
Name: Eric E. Trader
Title: Associate Privacy Officer
Email: oig_privacy@doioig.gov
Phone: 202-208-1644
Address: 1849 C Street, NW, MS-4428-MIB, Washington DC, 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on

- ☐ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☒ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Office of Inspector General (OIG) General Support System (GSS) system (OIG-GSS) is composed of network computing hardware and related software in support of network management and storage capabilities via OIG network shared drives and OIG-furnished laptops, voice over internet protocol services, active directory management, and file system management. The OIG-GSS supports the OIG's oversight and investigative responsibilities and helps OIG

manage criminal, civil, and administrative investigations of fraud, waste, and abuse in programs administered by the Department of the Interior (DOI), perform audit management and assignment of personnel, and inspections in accordance with generally accepted government auditing standards and other policies.

The key services 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 storages and backup for disaster recovery
- Voice-over-IP infrastructure
- Personal computing and mobile devices
- Wireless access points
- Data-at-rest and data-in-transit encryption capabilities
- Virtual collaboration tools

In addition to the services supporting the OIG-GSS, there are six (6) minor applications that reside within OIG's GSS security boundary, which are the following:

- AMP - a workflow management application that provides operational support across OIG offices, which includes functions such as work scheduling, small procurement (typically items/services less than $5,000), on-boarding/off-boarding employees, Performance Award, etc.
- Case Management System (CMS) - a web-based system used by the Office of Investigations (OI) within the OIG that tracks complaints, preliminary inquiries, and investigations that OIG Staff use for case management and program referral capabilities. The system is designed to facilitate criminal, civil, and administrative investigations of fraud, waste, and abuse in programs administered by the DOI. The CMS is designed to generate statutorily required information and management reports, as well as assisting in the overall management and collection of data that is required for successful prosecutions.
- Customer Service Portal (CSP) - 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, IT In & Out Process, AIE Helpdesk, Facility Helpdesk, Financial Management Helpdesk, FOS Device property, IT Equipment, IT Helpdesk, IT Security Helpdesk, OI Helpdesk, and Office of General Counsel

Helpdesk. Access to those systems are limited to those employees with appropriate authorization.

- Hub 2.0 – OIG Intranet site for information sharing to its employees, which includes operational announcements, references to job aids, organizational charts and an employee directory.
- Nuix - a web-based, commercial-off-the-shelf (COTS) product that makes evidence data securely and conveniently available to its users. It will be managed by the DOI OIG OI. The Information Technology Division (ITD) will be its primary contact for system administration functions.
- TeamMate - a commercial off-the shelf software application designed to control audit planning, fieldwork, collaboration, review, reporting, resolution, follow-up, and efficiency. Data is captured into a centralized database managed by OIG. TeamMate data is accessible over the OIG network through client application connections to the centralized database. TeamMate 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.

This PIA covers the OIG-GSS and the minor applications.

C. What is the legal authority?

The nature and scope of OIG's oversight and investigative responsibilities are established and set forth in 5 U.S.C App. Inspector General Act of 1978, as Amended. In order to enable OIG to perform its oversight and investigative functions, the Inspector General Act of 1978 authorizes OIG to have access to "all record, 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.

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☒ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

UII Code: 010-000002258; System Security and Privacy Plan for the Office of Inspector General-General Support System (OIG-GSS)

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
AMP	This is a workflow management application that provides operational support across OIG offices including work scheduling, small procurement, employee on-boarding/off-boarding, Performance Award, etc.	Yes	Employee Full name, Personal Email Address, Home Phone Number, Home Mailing Address, Emergency Contact
Case Management System (CMS)	This application is used by the Office of Investigations within the OIG that tracks complaints, preliminary inquiries, and investigations that OIG Staff use for case management and program referral capabilities. The system is designed to facilitate criminal, civil, and administrative investigations of fraud, waste, and abuse in programs administered by the DOI.	Yes	Full name, Citizenship, Gender, Birth Date, Other Names Used, Place of Birth, Driver's License, Social Security Number, Tribal or Other ID Number, Personal Email Address, Home Telephone Number, Employment Information, and Mailing/Home Address, Race/Ethnicity, Group Affiliation, Medical Information. Any other PII necessary to conduct the criminal, civil, and/or administrative investigation covered under SORN Investigative Records - Interior, OIG-2.

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
Customer Service Portal (CSP)	This is an OIG enterprise-wide and designed to be accessible only by OIG employees. Inherent in the OIG Customer Service Portal are the following applications: Correspondence Tracking System (CTS), Employee List, IT In & Out Process, AIE Helpdesk, Facility Helpdesk, Financial Management Helpdesk, FOS Device property, IT Equipment, IT Helpdesk, IT Security Helpdesk, OI Helpdesk, and Office of General Counsel Helpdesk. Access to those systems are limited to those employees with appropriate authorization.	Yes	Employee full name, Office assignment, location, and phone numbers, and Employee Email Address
Hub 2.0	OIG Intranet site for information sharing to its employees. Although an employees' PII is collected for official business purposes, within the OIG Employee Directory, employees may voluntarily provide personal information about themselves or their family as part of their respective employee profile story. All voluntarily provided information is reviewed by an OIG writer/editor and employees must	Yes	Employee full name, Employee Email Address, Education Information, Employment Information, Marital Status, Spouse Information, Child/Dependent Information, Race/Ethnicity (via uploaded images/pictures voluntarily provided by the employee), Military Status/Service

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
	consent to disclosing the voluntarily provided information.		
Nuix	This minor application stores and makes evidence data securely and conveniently available to its users.	Yes	Full name, Citizenship, Social Security Number, Gender, Date of Birth, Spouse Information, Personal Email Address, Home Mailing Address, Home Phone Number, Driver's License, Race/Ethnicity. Any other PII necessary to conduct the criminal, civil, and/or administrative investigation covered under SORN Investigative Records - Interior, OIG-2.
TeamMate	This minor application is designed to control audit planning, fieldwork, collaboration, review, reporting, resolution, follow-up, and efficiency. Data is captured into a centralized database managed by OIG. TeamMate data is accessible over the OIG network through client application connections to the centralized database. TeamMate is OIG's database for electronic audit, inspection, and quality control review project files. The purpose is to facilitate audit management and assignments of	Yes	Full name, Social Security Number, Gender, Date of Birth, Personal Email Address, Financial Information, Credit Card Number

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
	personnel, and document audits and inspections in accordance with generally accepted government auditing standards and other policies.		

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

Due to the nature of the OIG GSS, there may be numerous programs, applications and systems that collect, maintain or process PII and are under the control and ownership of a system owner, information owner, or Privacy Act system manager who are responsible for meeting the requirements of the Privacy Act.

Audit records are maintained under OIG-1, Management Information, 55 FR 14480, April 18, 1990.

OIG investigations and case file records are covered under OIG-2, Investigative Records - 76 FR 60519, September 29, 2011. DOI published regulations at 43 CFR part 2, subpart K to exempt certain records in OIG-2 from some provisions of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

General employee personnel records are maintained under Office of Personnel and Management (OPM) government-wide notices including OPM/GOVT-1, General Personnel Records, 77 FR 73694 (December 11, 2012); modification published at 80 FR 74815 (November 30, 2015).

General administrative records are maintained under DOI-58, Employee Administrative Records - 64 FR 19384, April 20, 1999, Modification published 73 FR 8342, February 13, 2008.

Active Directory user accounts are covered under DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) - March 12, 2007, 72 FR 11040.

DOI SORNs may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn.

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☐ Yes: *Describe*
☒ No

OIG Hotline has four forms: https://www.doioig.gov/oig-hotline-forms

- Hotline Complaint Form: https://forms.doioig.gov/(S(3z2bv0wctvchruwb3e43rdrw))/hotlinecomplaint_general_form.aspx
- Confidential Hotline Complaint Form: https://forms.doioig.gov/(S(ygqqjk335qezrf40zb0swiqj))/hotlinecomplaint_confidential_form.aspx
- Anonymous Hotline Complaint Form: https://forms.doioig.gov/(S(ylia0pl1mwrhrd5sbmr5k5ag))/hotlinecomplaint_annoymouse_form.aspx
- Whistleblower Reprisal Complaint Form: https://forms.doioig.gov/(S(4m3il50huycqhgh2xmmeo4we))/hotlinecomplaint_whistleblower_form.aspx

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name	☒ Religious Preference	☒ Social Security Number (SSN)
☒ Citizenship	☒ Security Clearance	☒ Personal Cell Telephone Number
☒ Gender	☒ Spouse Information	☒ Tribal or Other ID Number
☒ Birth Date	☒ Financial Information	☒ Personal Email Address
☒ Group Affiliation	☒ Medical Information	☒ Mother's Maiden Name
☒ Marital Status	☒ Disability Information	☒ Home Telephone Number
☒ Biometrics	☒ Credit Card Number	☒ Child or Dependent Information
☒ Other Names Used	☒ Law Enforcement	☒ Employment Information
☒ Truncated SSN	☒ Education Information	☒ Military Status/Service
☒ Legal Status	☒ Emergency Contact	☒ Mailing/Home Address
☒ Place of Birth	☒ Driver's License	☒ Race/Ethnicity

☒ Other: *Specify the PII collected.*

This system may contain and/or use data such as emails, documents, spreadsheets, law enforcement incident reports, personnel records, and other employee sensitive information (ESI) as outlined in the table of applications in question F above.

Records may be created and used by 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; to conduct audits of DOI programs and operations; to maintain records related to the OIG's activities; and fulfill reporting requirements to DOI and its components, Congress, the Department of Justice, the public and other entities. These activities may require a broad scope of personally identifiable information (PII) about individuals that may include: SSNs, driver's license numbers, credit card numbers, vehicle identification numbers, license plate numbers, names, home addresses, work addresses, telephone numbers, email addresses and other contact information, emergency contact information, ethnicity and race, tribal identification numbers or other tribal enrollment data, work history, educational history, affiliations, and other related data, dates of birth, places of birth, passport numbers, gender, and other physical or distinguishing attributes of an individual.

Additionally, applications such as CMS and Nuix may contain images from videos collected from digital devices or audio/visual recording devices such as surveillance cameras, including closed circuit television located at DOI facilities for security and/or law enforcement operations. Data and investigative reports in the system may include attachments such as photos, audio recordings, sketches, medical reports, text messages, and information concerning criminal activity, response, outcomes, as well as, any other information gathered during investigations.

CMS, Nuix, and/or the Office of Investigations records may also include information concerning Federal civilian employees and contractors, Federal, tribal, state and local law enforcement officers and may contain information regarding an officer's name, contact information, station and career history, firearms qualifications, medical history, background investigation and status, date of birth and SSN.

As data is turned over to or captured by the DOI OIG, any number of possible PII data points could be included in that data. These examples may not represent all the possible PII that may incidentally be collected by DOI OIG during an investigation.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☒ Federal agency
☒ Tribal agency
☒ Local agency
☒ DOI records
☒ Third party source
☒ State agency
☒ Other: *Describe*

Information input into the system is collected through Department records requests, subpoenas, search warrants, seizure of evidence, and voluntary disclosure. These sources of information are acquired from investigative activities authorized by the Inspector General Act of 1978 as Amended.

C. How will the information be collected? Indicate all that apply.

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

Data may be collected from telephone, text message, or email records obtained from cellular carriers, internet service providers, and other companies. Information may also be obtained from public access web sites, newspapers, press releases, or other sources. Information may also be obtained through data feeds to other Law Enforcement databases or systems. Information may be derived from other Federal systems to share information across the Law Enforcement community. Overall, data is collected through investigative activities including, but not limited to: subpoenas, search warrants, evidence seizure, DOI records requests, and voluntary disclosure.

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

The primary use of the records 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 charge card number and other PII in audits involving the integrated charge card program.

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

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

- For AMP, PII may be shared within the DOI OIG for workflow management operational support such as work scheduling, employee onboarding/offboarding checklist/guides, small procurement activities, performance awards, storing/viewing employee agreements or records, and report generation.
- For the HUB 2.0, PII may be shared within the DOI OIG to search and identify OIG personnel and it is used as an employee directory. All data within the system is open to all OIG employees. Although an employees' PII is collected for official business purposes, within the OIG Employee Directory, employees may voluntarily provide personal information about themselves or their family as part of their respective employee profile story. All voluntarily provided information is reviewed by an OIG writer/editor and employees must consent to disclosing the voluntarily provided information.
- For CSP, PII may be shared within OGC ITD to identify individuals through the CTS, such as, submitters of helpdesk requests, and identify employees issued government furnished equipment (GFE).
- 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 those authorized and holding appropriate security clearances.
- For Nuix, PII may be shared with authorized users within DOI OIG as part of the investigative process. Access to the Nuix system itself is strictly limited within the OIG to those with approval.
- For TeamMate, PII may be shared within the Audits, Inspections, and Evaluation (AIE) team as well as OI.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

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

It is possible that OIG may share PII with the 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 Federal Personnel and Payroll System, O365, SharePoint, Teams, etc., which are not within scope of this PIA and have been evaluated under separate DOI PIAs.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

PII may be shared with the U.S. Attorney's Office or other Federal agencies that are part of an OIG or joint investigation 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 the system of records notice OIG-2, Investigative Records, 76 FR 60519, September 29, 2011 which may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn. Law enforcement records are exempt under 5 U.S.C. 552a(j)(2) and (k)(2).

PII from other minor applications are only shared to the extent authorized under the Privacy Act and published routine uses in applicable government-wide and DOI SORNs.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

PII may be shared with other 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 contained in CMS may be disclosed outside OIG as a routine use pursuant to 5 U.S.C. 552a(b)(3), published in the system of records notice OIG-2, Investigative Records, 76 FR 60519, September 29, 2011 which may be viewed on the DOI SORN website at https://www.doi.gov/privacy/doi-notices. Law enforcement records are exempt under 5 U.S.C. 552a(j)(2) and (k)(2).

PII from other minor applications are only shared to the extent authorized under the Privacy Act and published routine uses in applicable government-wide and DOI SORNs.

☒ Contractor: *Describe the contractor and how the data will be used.*

OIG has contractors who are authorized to perform system development support for minor applications such as AMP, CMS and the HUB 2.0.

☒ Other Third Party Sources: *Describe the third party source and how the data will be used.*

PII may be shared with any Third-Party source 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 contained in CMS may be disclosed outside OIG as a routine use pursuant to 5 U.S.C. 552a(b)(3), published in the system of records notice OIG-2, Investigative Records, 76 FR 60519, September 29, 2011 which may be viewed on the DOI SORN website at https://www.doi.gov/privacy/doi-notices. Law enforcement records are exempt under 5 U.S.C. 552a(j)(2) and (k)(2).

PII from other minor applications are only shared to the extent authorized under the Privacy Act and published routine uses in applicable government-wide and DOI SORNs.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Within the employee directory of HUB 2.0, OIG employees may voluntarily provide personal information within their respective employee profile page or decline to provide such information, e.g., family fun photos that individual employees can either intentionally share with the rest of the organization or choose to opt-out.

☒ 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, 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. In some cases, individual members of the public may decline to provide information where providing information is voluntary; and are informed of this right by authorized OIG staff. For employees who use DOI email, DOI owned electronic assets, and use of audio and visual recordings, and for individuals who enter on Federal properties and public areas, there is no reasonable expectation of privacy. Individuals who use the DOI network must acknowledge a warning that advises them that the network is monitored. 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. Information obtained by various legal process methodologies may also be without the knowledge of those whom the record relates to.

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ Privacy Act Statement: *Describe each applicable format.*

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through the publication of this privacy impact assessment and the publication of the other related SORNs referenced above which may be viewed on the DOI SORN website at https://www.doi.gov/privacy/os-notices. Law enforcement records are exempt under 5 U.S.C. 552a(j)(2) and (k)(2).

The OIG website contains a Privacy Policy that describes how OIG uses PII that is submitted by individuals through a complaint or online form: https://www.doioig.gov/privacy. Individuals are advised of their rights on the Complaint Hotline page which includes an Information Disclosure and Privacy Act Notice.

☒ Other: *Describe each applicable format.*

In some cases, such as for Departmental email and electronic devices, or use of audio and visual recordings, individuals who enter on Federal properties and public areas do not have a reasonable expectation of privacy. Users of the DOI network are provided a security warning banner when accessing the network that advises them that the user activities may be monitored for security purposes. 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.

☐ None

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

Regarding Nuix, 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 data in the system. Data can also be automatically filtered by date/time, file type, or other file metadata non-specific to an individual.

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

The HUB contains an OIG employee directory in which information can be retrieved by searching a person's first or last name.

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 or telework agreements submitted by a specific employee. Or a report could be run to show all work schedules or telework agreements submitted in a specific year.

CSP data is retrieved by system generated request reference number. Only OIG authorized employees/administrators can access request data. The reference number is used to retrieve relevant request data by OIG administrators for OIG internal use.

TeamMate data is generally retrieved based upon assignment number and project name. Key word searches can be used within a project. Data is not retrieved based upon individually identifying information.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

Both CMS and Nuix applications have the capability to produce case-based reports involving information regarding a subject of an investigation. Cases are assigned to and accessed by a specific regional agent. The report(s) is used as supporting documentation of 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.

In addition to case-based reports, the OIG-GSS and most minor applications have auditing capabilities. Audit logs consist of user-based activity which often consists of 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 events such as login attempts (both successful and unsuccessful), password changes, objects accessed, and folders/files created, modified, or deleted are uniquely identified by username and each event is timestamped. Audit logs or reports are used for monitoring purposes in support of FISMA requirements as well as both change management and incident management process. Audit logs are only accessible by OIG ITD administrators or the application administrator.

☐ No

Section 3. Attributes of System Data

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

AMP, CSP and Hub 2.0 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. Nuix 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 in attempt to independently corroborate or verify the accuracy of data collected per OIG policy and procedures. Supervisors will also review data for accuracy. TeamMate, 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.

B. How will data be checked for completeness?

AMP and TeamMate, 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. PII is only retained if relevant to the request for service or the process being performed. 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 Nuix. Any information that is portrayed within

HUB 2.0 is often reviewed by writers/editors from the OIG's Communications and Reports Unit or by an office representative before being published on the website.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

Nuix will be used to analyze historical data as opposed to real time or current data. Overall, individual users, including supervisors, are responsible for ensuring the data is accurate for analysis purposes. This may be done by validation with applicable law enforcement systems, CMS, and various investigative processes that are designed to determine or ensuring information is current.

The TeamMate Data Owner is responsible for reviewing and updating PII records such as credit card numbers and other financial information.

With regards to all other minor applications such as AMP, CSP, and HUB 2.0 on the OIG-GSS, there is no process to maintain current data unless the user submits a service ticket to request a name change in Human Resources and in Active Directory.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

The OIG complies with the OIG and the Office of the Secretary (OS) Records Disposal Schedule (RDS). For example, work schedule and telework agreement records are maintained in accordance with the records schedule for personnel records, SF-1164 Claim for Reimbursement records are kept in accordance with the records schedule for finance records. CSP retains records for ten years.

Nuix records are retained and dispositioned in accordance with OS, RDS, 2802 - Investigative Records, which was approved by the National Archives and Records Administration (NARA) (N1-048-10-03). 2802.1 Investigation Records Selected for their Continuing Historical Value disposition is Permanent. The record is cut off at end of fiscal year in which the investigation is concluded. Records are transfer to NARA 25 years after cut-off. 2802.2 All Other Investigative Records disposition is Temporary. The record is cut off at end of fiscal year in which the investigation is concluded. Records are destroyed 10 years after cut off.

CMS records are retained and dispositioned in accordance with OS, RDS, 2802 - Investigative Records, which was approved by NARA (N1-048-10-03). 2802.1 Investigation Records Selected for their Continuing Historical Value disposition is Permanent. The record is cut off at end of fiscal year in which the investigation is concluded. Records are transfer to NARA 25 years after cut-off. 2802.2 All Other Investigative Records disposition is Temporary. The record is cut off at end of fiscal year in which the investigation is concluded. Records are destroyed 10 years after cut off.

TeamMate records are retained and dispositioned in accordance with OS, RDS, 1210 - Audit Files, which was approved by NARA (N1-048-08-22). 1210.3 Other Audits disposition is Temporary. Cut off when the final audit report is made. Records are destroyed 7 years after cut off.

HUB 2.0 records are retained and dispositioned in accordance with OS, RDS, 1217 - Website Files. Cut off when data is superseded. Records are destroyed when no longer needed for agency business. (DRS 1.4.0013, DAA-0048-2013-0001-0013)

AMP records are retained and dispositioned in accordance with several OS, RDS depending on the nature of the records. 1102 - General Administration Files disposition is Temporary. Cut off record at the end of the fiscal year in which the record is created. Records are destroyed 3 years after cut-off. (DRS 1.1.0001 DAA-0048-2013-0001-0001). 1110 - Routine Procurement Files disposition is Temporary. Cut off on final payment. Records are destroyed 7 years after cut-off. (DRS 1.3.0011 DAA-0048 2013-0001-0011). 1304.1 - Agency Training disposition is Temporary. Cut off record at end of fiscal year in which files are closed. Records are destroyed 7 years after cut-off. (DRS 1.2.0005 DAA-0048-2013-0001-0005). 1304.2 - Employee Training disposition is Temporary. Cut off when superseded or obsolete. Records are destroyed 7 years after cut-off. (DRS 1.2.0005 DAA-0048-2013-0001-0005). 1305.1- Agency Awards disposition is Temporary. Cut off on approval or disapproval of award. Records are destroyed 3 years after cut-off. (DRS 1.2.0004 DAA-0048-2013-0001-0004).

CSP records are retained and dispositioned in accordance with 1106 - Tracking and Control Files disposition is Temporary. Cut off after the date of the latest entry. Destroy when no longer needed. (DRS 1.1.0003 DAA-0048-2013-0001-0003).

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Proponent offices (Division of Human Resources, Division of Financial Management, Facilities and Operations Support, Office of Investigations (OI), etc.) coordinate with the system administrator and OIG Records Officer to review records, authorize destruction, and purge records which have reached or passed their retention period. This is usually accomplished at the beginning of each new FY.

Archival and disposition of records will follow applicable guidance by NARA, applicable legislation such as the Federal Records Act, and Departmental guidance. Permanent records are cut off at the end of the fiscal year in which the investigation is concluded and transferred to NARA 25 years after cut-off. Approved disposition methods for temporary records include shredding for paper records, and erasing for electronic records, in accordance with NARA guidelines and DOI and OIG records disposition requirements.

With respect to the TeamMate application, the archive feature will be used to remove records from the central database to an archive database. After supervisory review, the archive database will be deleted.

As for the HUB 2.0, employee data is removed from the employee directory after the employee leaves OIG.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a moderate risk to the privacy of individuals due to the amount of sensitive PII maintained for law enforcement incident reports, law enforcement investigations, etc. The risks are mitigated by controls implemented to limit unauthorized exposure of PII. Only authorized personnel with proper credentials can access the records in the system. DOI OIG requires two-factor authentication for network and system access; system access is based on least privilege access and role-based access controls; access control lists were created and segmented by OIG office; users cannot view information for other users unless specifically authorized. Furthermore, OI implements and enforces policies and procedures concerning the protection and disclosure of investigative information. 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. At the server level, successful and unsuccessful login attempts are logged.

Privacy risks include but are not limited to unauthorized access to or dissemination of data containing PII, personal/business financial information, sensitive business information, and intellectual property.

The data is protected through the various stages of the information lifecycle:

- Notice - There is a risk that individuals may not have adequate notice. This PIA and the published SORNs described in Section 1, Question G above provides constructive notice. Note that DOI claimed Privacy Act exemptions for records maintained under OIG-2 pursuant to 5 U.S.C. 552a(j)(2) and (k)(2) that may preclude individual notice in order to protect law enforcement investigations.
- Collection – Only data that is pertinent to the OIG mission is collected. Any collection of PII has been appropriately sanctioned and referenced within the corresponding SORNs described in Section 1, Question G above.
- Use – The OIG-GSS and its minor applications are internal, non-public facing information systems. Only DOI OIG employees may have access to data on a "need-to-know" basis. However, investigative case information may be shared with other DOI offices, and law enforcement or prosecutive agencies as needed. PII is used for its intended purpose in support of the OIG mission.

- Retention – The OIG-GSS and its minor applications maintain all records with PII in accordance with applicable records retention or disposition schedules approved by the National Archives and Records Administration (NARA) or based on the need and relevancy of the data in the support of the OIG mission. Regarding Nuix, there is a risk that the system may collect, store or share more information than necessary, or the information will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule.
- Processing – The OIG-GSS and its minor applications are internal, non-public facing information systems. Data can only be processed and is accessible from DOI OIG government-furnished equipment (GFE).
- Disclosure – PII and other sensitive information is protected from unauthorized disclosure using the following methods:
    - Role-based access, rights and permissions
        - Regarding the OIG-GSS and its minor applications, users only have access to information that is necessary to perform their duties or job function as well as a need-to-know basis.
    - Encryption
        - Data In-Transit: TLS 1.2, 256-bit encrypted connections using a SSL PKI DOI certificate with an approved web browser
        - Data In-Use: On-screen masking or abbreviation
        - Data At-Rest:
            - Windows workstations and laptops with encryption tool installed
            - Windows servers and virtualized hosts with encryption to protect data-at-rest
            - USB encrypted thumb and hard disk drives

  There are also privacy risks when sharing data with other law enforcement organizations related to the unauthorized sharing, data integrity or loss of data. Disclosure of sensitive information is made as defined in Section 2(D) of this document. Investigative information is highly protected and available for disclosure only by certain officials within OI and external organization only for authorized purposes. The authorized sharing of information in support of law enforcement activities is described in the routine uses published in the OIG-2 SORN.

- Destruction – DOI policy and records retention schedules dictate proper disposal of records at the end of the retention period and records are disposed of in accordance with NARA approved records schedules. Permanent records are transferred to NARA. Temporary records are deleted from the system by a designated technician at the request of the case agent or the close of the case. Any data that has been deemed obsolete or no longer needed is purged from the information system.

Due to the nature of law enforcement investigations, data collected about individuals from sources may be aggregated during the course of an investigation. There is a risk that data from different sources may be aggregated and may provide more information about an individual.

There is a risk that individuals may not know how to seek redress or correction of their records. Individuals seeking redress may submit requests for correction through established procedures outlined in DOI Privacy Act regulations at 43 CFR 2.246 and in the applicable published SORN. The DOI Privacy and Civil Liberties web page at https://www.doi.gov/privacy/privacy-civil-liberties also provides information on how individuals may submit a complaint or a request to correct erroneous information. However, DOI has exempted law enforcement records in the OIG-2 system of records from one or more provisions of the Privacy Act under 5 U.S.C. 552a(j)(2) and (k)(2), in order to preclude an individual subject's access to and amendment of information or records related to or in support of an investigation.

OIG-GSS is rated as a FISMA moderate system based upon the type and sensitivity of data and requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive data contained in the system. The privacy controls are utilized to protect individual privacy, including limiting access to images or video feed that identify individuals or to specific events or investigations that are linked to individuals, to authorized users and law enforcement officials, and establishing controls on the retention of images and video feeds to the approved period necessary for law enforcement purposes in accordance with approved records retention schedules.

DOI OIG employees and contractors must take privacy, security and records management training prior to being granted access to DOI information and information systems, and annually thereafter. Personnel with significant privacy responsibilities, such as law enforcement personnel, must also take role-based privacy training initially and annually, to ensure an understanding of the responsibility to protect privacy. Failure to protect PII or mishandling or misuse of PII may result in criminal, civil, and administrative penalties.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

The use of PII is relevant and necessary for the purpose of performing required administrative and functional operations to comply with an audit, and while 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. This supports DOI OIG investigative and law enforcement activities in accordance with the Inspector General Act of 1978, as amended.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☒ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

With regards to the Nuix application, the system is capable of producing communication network diagrams, timelines, and charts from statistical information of the types/categories of artifacts within the data set. Nuix 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. With respect to TeamMate, employee charge card data is updated. In terms of CMS, new data for investigative reports regarding a subject may be derived from external sources such as interviews, social media, or other system applications. For the HUB 2.0, new records are derived from Human Resources as new employees join the OIG. Also, an employee profile is created based on direct input from the employee with his or her consent to publish information on the intranet website.

☐ No

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

☒ Yes: *Explanation*

With regards to the Nuix application, results of analysis or reports may lead to being included in the individual's record as necessary and required for OIG investigations. In terms of AMP, new data for employees may include items such as awards and updated work schedules and telework agreement records. With respect to CMS, new data or evidence may be updated in a subject's case file.

☐ No

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

☒ Yes: *Explanation*

The Nuix application supports OIG investigative activities, which may include investigations or reports that result in determinations about individuals. Reports or results of investigations may be shared internally and externally as authorized and necessary to meet criminal, civil and administrative law enforcement requirements, as outlined above in Section 2, question E, and the routine uses in the published OIG-2, Investigative Records, 76 FR 60519, September 29, 2011 which may be viewed on the

DOI SORN website at https://www.doi.gov/privacy/doi-notices.

☐ No

E. How will the new data be verified for relevance and accuracy?

Regarding both CMS and Nuix applications, OIG agents and analysts and their supervisors are responsible for the relevance and corroboration of any data identified as relevant to an investigation. Data is validated through investigative means. Nuix cannot check for accuracy of the information but it does enforce the use of correctly formatted data. TeamMate data is reviewed and verified based on the financial information on file. In terms of the HUB 2.0, new employee information is verified for relevance and accuracy based on records from Human Resources or by contacting or interviewing the employee.

F. Are the data or the processes being consolidated?

☒ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

For the purposes of AMP, CSP, and Nuix, data is consolidated in management level reports for the purpose of assessing system and process performance and for resolving user issues. Technical controls at the application, server, and network level exist to prevent unauthorized access. Only OIG authorized employees/administrators can access data and run reports. All other minor applications do not consolidate data.

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

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

Each application is internally-facing, so users must first provide multifactor authentication (PIV card "something you have" and a PIN "something you know") in order to access these applications. Remote access to data is protected via virtual private network (VPN). Data in transit is encrypted by a DOI SSL PKI certificate with TLS 1.2 encryption, 256-bit Advance Encryption Standard (AES) hashing algorithm. Developers have a separate administrative

account to obtain privileged access to systems and its data. Access is protected via Secure Shell (SSH).

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Access is restricted based upon need-to-know and OIG policy. Access is determined based upon Active Directory UserIDs and are set at both the system and project level. System level access is set by the System Administrator and is restricted to AI&E personnel (with some very limited exceptions). To access a specific project, a user must either be assigned to that project or be a member of a security group with read access to that project. Sensitive projects (such as those containing PII) are restricted to those directly assigned to the project and to headquarters management. In addition, specific documents within an assignment can be marked confidential which will restrict access to those with the same or higher access level. The system logs who has accessed particular projects and who has edited (but not accessed) particular documents within a project.

Users will be given access based on management approval for an official request. User access is restricted to data relevant to the case for which the request was generated and approved (see response above in F for further access controls). Furthermore, data sets can be compartmentalized to further restrict access to subsets of the data when applicable.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Contractors are involved with AMP, CMS, and the HUB 2.0 only, and are subject to the same requirements and standards as federal employees.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*

☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

System logs are present. 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. For example, who edited a record is logged, but not the specific changes made.

Additionally, the minor applications provide the system the capability to identify and locate individuals. Data collected may include physical attributes of an individual (including text, photos, and video), home and work addresses, phone numbers, and email addresses, as well as, other individuals and associations related to the individual.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

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. Logs capture who edited a record, but not any specific changes that were made.

M. What controls will be used to prevent unauthorized monitoring?

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 and DOI Guidance and Policies. Users are required to acknowledge and comply with the Rules of Behavior agreement.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☒ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☒ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices

☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☒ Other. *Describe*

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.

(3) Administrative Controls. Indicate all that apply.

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

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The IT Director, Information Technology Division is the Information System Owner for OIG-GSS who is the official responsible for oversight and management of the OIG-GSS security controls and the protection of information processed and stored by the OIG-GSS. Each minor application has an assigned a data owner / system owner who has the overall responsibility for protecting the data. In coordination with the OIG Associate Privacy

Officer, the data owner or system owner is responsible for protecting the privacy rights of individuals whose personal data may be contained in this system. The Information System Owner, Information System Security Officer, and authorized users are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored within the applications, and coordinating Privacy Act requests for notification, access, amendment, and complaints with the Privacy Act System Managers in consultation with DOI Privacy Officials, OIG senior leadership, and the OIG General Counsel.

P. 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 or data owner, data custodian, and the information system security officer are responsible for assuring proper use of data and reporting to the agency/bureau privacy the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information. All authorized users are responsible for reporting any compromising, suspected or confirmed breach of data to DOI-CIRC, DOI's incident report portal, within one hour of discovery.