**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 Secure File and Collaboration Portal (OSFCP)
**Bureau/Office:** Office of Inspector General (OIG)
**Date:** September 26, 2022
**Point of Contact**
Name: Eric 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:

### B. What is the purpose of the system?

OIG Secure File and Collaboration Portal (OSFCP) is a web application used for the purpose of exchanging large-sized files and collaborating with law enforcement organizations on an individual investigative case in a secure manner. Since OSFCP has both internal users managed by OIG and external law enforcement agency users, the web application is publicly accessible but may only be accessed by authorized officials. OSFCP is a software-as-a-service (SaaS)

solution which is provided by Box for Government - a FedRAMP authorized cloud service provider. Box's networking and storage environment is controlled by Amazon Web Services (AWS) cloud as the Infrastructure as a Service (IaaS) cloud service provider. The Department of the Interior (DOI) OIG is responsible for all account management activities, secure configuration of the application, establishing access controls, and content management activities.

**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:

**E. Is this information system registered in CSAM?**

☒ Yes:

UII Code: 010-000002809; OSFCP System Security and Privacy Plan

☐ 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.* |
|---|---|---|---|
| None | None | No | N/A |

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

☒ Yes:

INTERIOR/OIG-2, Investigative Records - 76 FR 60519, September 29, 2011, modification published at 86 FR 50156, September 7, 2021. 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).

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

These 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:

☒ No

## Section 2. Summary of System Data

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

☒ Name
☒ Citizenship
☒ Gender
☒ Birth Date
☒ Group Affiliation
☒ Marital Status
☒ Biometrics
☒ Other Names Used
☒ Truncated SSN
☒ Legal Status
☒ Place of Birth
☒ Religious Preference
☒ Security Clearance

☒ Spouse Information
☒ Financial Information
☒ Medical Information
☒ Disability Information
☒ Credit Card Number
☒ Law Enforcement
☒ Education Information
☒ Emergency Contact
☒ Driver's License
☒ Race/Ethnicity
☒ Social Security Number (SSN)
☒ Personal Cell Telephone Number
☒ Tribal or Other ID Number
☒ Personal Email Address
☒ Mother's Maiden Name
☒ Home Telephone Number
☒ Child or Dependent Information
☒ Employment Information
☒ Military Status/Service
☒ Mailing/Home Address
☒ Other:

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). 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 (DOJ), 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.

The system may also contain images and 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 in the system may include attachments such as photos, video, sketches, medical reports, text

messages, and information concerning criminal activity, response, outcomes, as well as, any other information gathered during investigations.

Additionally, 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 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 OIG during an investigation.

OIG employees use their government issued Personal Identity Verification (PIV) card authenticated through the Enterprise Active Directory to log in to the OSFCP portal. External law enforcement users are required to provide a Username and Password to create an account and access the system. These external users may use a mobile authenticator application, such as Microsoft Authenticator or Google Authenticator, or short messaging service (SMS) text code for authentication purposes. Internal and external users' email addresses are also collected to create an account and to facilitate any sharing of information or collaboration with OIG.

**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:

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. Information is collected from the external law enforcement users to create an account and to share information or collaborate with OIG.

**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:
☒ Other:

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 DOJ, the public and other entities as appropriate within the mission of the OIG.

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

☒ Within the Bureau/Office:

PII within this system may be shared with authorized personnel within the OIG as part of the investigative or report development process. Access to information is restricted to those authorized and holding appropriate security clearances.

☒ Other Bureaus/Offices:

PII within this system may be shared with the Office of the Secretary (OS) or other bureaus only to the extent necessary to carry out OIG investigations and reporting requirements pursuant to the Inspector General Act. Access to information is strictly limited to those authorized by the OIG.

☒ Other Federal Agencies:

PII may be shared with the U.S. Attorney's Office, Federal law enforcement agencies 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 SORN, OIG-2, Investigative Records, 76 FR 60519, September 29, 2011, modification published at 86 FR 50156, September 7, 2021, 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).

☒ Tribal, State or Local Agencies:

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 may be disclosed outside OIG as a routine use pursuant to 5 U.S.C. 552a(b)(3), published in the SORN, OIG-2, Investigative Records, 76 FR 60519, September 29, 2011, modification published at 86 FR 50156, September 7, 2021, 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).

☒ Contractor:

Under atypical and extraordinary circumstances, PII may be disclosed to the vendor when explicitly authorized to provide technical support to the OSFCP. Examples of such circumstances are limited to situations like investigating an unforeseen security breach – even including an employee of the cloud service provider and whenever there is an issue of data corruption which requires approved and intentional troubleshooting activities on behalf of the cloud service provider.

☒ Other Third Party Sources:

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 may be disclosed outside OIG as a routine use pursuant to 5 U.S.C. 552a(b)(3), published in the SORN, OIG-2, Investigative Records, 76 FR 60519, September 29, 2011, modification published at 86 FR 50156, September 7, 2021, 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).

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

☐ Yes:

☒ No:

Due to the purpose and nature of the system and to help facilitate the OIG's law enforcement investigations, 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 procured cloud-based services such as the OSFCP web application, 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 OSFCP web application or any other DOI network must acknowledge a warning that advises them that the information system and/or 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:

☒ Privacy Notice:

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:

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 OSFCP web application and 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.).**

Data will be retrieved by querying for specific files or folders by an individual's name or case number using the on-screen Search Box. However, users will only be able to search and view content for which they have been explicitly granted access.

**I. Will reports be produced on individuals?**

☒ Yes:

The OSFCP web application is only capable of producing user activity reports – based on manager users and external users. The user's name and email address are captured within the user activity report, which is vital for auditing purposes and to support OIG's continuous monitoring and incident response process if necessary.

Otherwise, the OSFCP web application does not produce reports on subjects of an investigation and does not by default produce a separate report focused on any individual. In summary, the OSFCP web application itself does not produce separate investigative reports that do not already exist independently in other information systems such as the OIG Case Management System (CMS) or in other OIG evidence files.

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 the Federal Information Security Modernization Act (FISMA) requirements as well as both change management and incident management process. Audit logs are only accessible by OIG Information Technology Division (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?**

Data is verified for accuracy by the individual collecting the data per OIG Office of Investigations (OI) policy and procedures. Supervisors will also review the data for accuracy.

**B. How will data be checked for completeness?**

OIG personnel within the OI will verify the completeness of data collected per OIG policy and procedures. Supervisors will also review data for completeness.

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

OSFCP 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.

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

OSFCP is not intended to be a permanent file repository. OIG ITD has enforced a 30-day file retention policy which means that each file will have a 30-day storage life from the upload date. After 30 days, files are automatically removed from a file owner's folder. File owner's may re-upload content if necessary. OSFCP managed users have been instructed that all original files or copies shall be maintained and stored within the OIG General Support System, specifically, OIG Network File Shares.

Investigative 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). The 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 transferred to NARA 25 years after cut-off. The 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.

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

OIG ITD has enforced a 30-day file retention policy which means that each file will have a 30-day storage life from the upload date. After 30 days, files are automatically removed from a file owner's folder and placed in the Trash Bin within the application. After 30-days, all files in the Trash Bin are permanently deleted and removed from the application.

OI coordinates 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.

**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 risk to the privacy of individuals due to the amount of sensitive PII maintained for law enforcement incident reports, law enforcement investigations, etc. 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. However, such risks are mitigated by the implementation of various security controls to limit unauthorized exposure of PII. While the OSFCP website is accessible on the Internet, only authorized personnel – including OIG internal or external partners – can access the records in the system by first receiving an email invitation to share and collaborate on selected folders and/or documents authorized by the content owner. Essentially, users cannot view information for other users unless specifically authorized. In addition, the OIG internal content owner has the option to specify external users to have either download, view, or edit permissions to authorized documents.

Also, DOI OIG requires two-factor authentication for both OIG internal users and external partners. OIG internal users are required to authenticate into OSFCP web application by using their OIG PIV card and typing the associated PIN. Meanwhile, external partners have the two options of multifactor authentication options: Username/Password along with either 1) mobile authenticator application, such as Microsoft Authenticator or Google Authenticator, or 2) SMS text code.

As another mitigating control, the administrative console has been configured to prevent external users from sharing OIG internally-owned content with other external users. Finally, our administrative console has been configured to block access to the web application from IP addresses and domains originating from certain countries outside of the United States, such as China, North Korea, Russia, etc.

Furthermore, OI implements and enforces policies and procedures concerning the protection and disclosure of investigative information. Additionally, OIG ITD has enforced a 30-day file retention policy which means that each file will have a 30-day storage life from the upload date. After 30 days, files are automatically removed from a file owner's folder and placed in the Trash

Bin within the application. After 30 days, all files in the Trash Bin are permanently deleted and removed from the application. The implementation of a file retention policy minimizes the impact of unauthorized disclosure in the event the system becomes compromised.

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. The collection is duplicated for use in the application by a forensic examiner/technician in a closed, alarmed, access-controlled lab on a stand-alone forensic computer before being transferred under the protection of the controls inherent in the OIG General Support System (OIG-GSS) to a controlled folder on the server running the application.
- Use – Data is processed on OIG-furnished laptops and can be uploaded and temporarily stored within the application. Web traffic between the end user and the cloud service provider's network infrastructure is encrypted and transmitted across the internet through transport layer security (TLS) 1.2 connections using an approved web browser. 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 – OSFCO maintains 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. 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. However, data within OSFCP is protected by the security controls provided by the cloud service provider and OIG's implementation of a 30-day file retention policy.
- Processing – Processing is performed by a special agent within the OI on an OIG furnished laptop.
- Disclosure – 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.

OSFCP 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.

As previously stated, OSFCP is a software-as-a-service (SaaS) solution which is provided by Box for Government - a FedRAMP authorized cloud service provider. Box's networking and storage environment is controlled by Amazon Web Services (AWS) cloud as the Infrastructure as a Service (IaaS) cloud service provider. The Department of the Interior (DOI) OIG is responsible for all account management activities, secure configuration of the application, establishing access controls, and content management activities. Meanwhile, Box as well as AWS are responsible for maintaining the underlying hardware and software applications and protecting the infrastructure which stores OIG data. To prevent unauthorized disclosure of OIG data, Box and AWS have deployed appropriate privileged access controls and data-at-rest encryption technologies to mitigate the risk to an acceptable level. The vendor does not have access to the PII in the system. However, there is a potential for authorized information disclosure. As previously mentioned, PII may be disclosed to the vendor under atypical and extraordinary circumstances, when explicitly authorized to provide technical support to the OSFCP. Examples of such circumstances are limited to situations like investigating an unforeseen security breach – even including an employee of the cloud service provider and whenever there is an issue of data corruption which requires approved and intentional troubleshooting activities on behalf of the cloud service provider.

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:

The use of PII within OSFCP is relevant and necessary 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:

OSFCP 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.

☐ No

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

☒ Yes:

Results of analysis or reports may lead to being included in the individual's record as necessary and required for OIG investigations and 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:

The OSFCP application support to 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 SORN, INTERIOR/OIG-2, Investigative Records, 76 FR 60519, September 29, 2011, modification published 86 FR 50156 (September 7, 2021) 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?**

OSFCP cannot check for accuracy of the information. OIG agents, 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.

**F. Are the data or the processes being consolidated?**

☒ Yes, data is being consolidated.

Unauthorized access to data contained in the system is protected through the controls of the OSFCP application, its administrator, and the cloud service provider by:

- Only authorized personnel with proper credentials/background investigation can access the system
- Least privilege access or permission sets
- Role-based access control
- 2-factor authentication into system
    - For internal OIG users: OIG PIV card and PIN
    - For external users: Username/Password and either mobile authenticator application, such as Microsoft Authenticator or Google Authenticator, or SMS text code

Users cannot view information for other users unless specifically authorized.

☒ Yes, processes are being consolidated.

To prevent unauthorized access to OIG data, the cloud service provider implements access control mechanisms for privileged users as well as data-at-rest encryption to protect our data while stored upon their infrastructure.

☐ 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:

External users who receive an invitation to collaborate and share with an internally managed user (e.g., OIG personnel).

**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. 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. When external users are granted access to collaborate and share, they can be given either Editor or Viewer permissions. The editor permission allows the recipient(s) to view and edit documents, while the viewer permission is basically "read-only." Print restrictions can also be enforced by the file content owner. Users cannot view information of other users unless specifically authorized.

**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.

As cloud service providers (CSPs), Box and AWS are responsible for maintaining the underlying hardware and software applications and protecting the infrastructure which stores OIG data. DOI OIG only has limited access to the configuration and administration of the service. Box requires a signed Security Addendum from any contractor who has a role which may require him or her access to Box Customer Content/Information or other sensitive data.

Both cloud service providers are FedRAMP-authorized which means that each CSP must comply with the requirements of the FedRAMP program and undergo security control assessments by a third-party assessment organization (3PAO) to maintain its status as an authorized vendor. Also, each CSP are subject to contractual obligations respective to each party. Services and the capabilities of Box (internally named as OSFCP) were designed to address both security and privacy-related concerns as it relates to 1452.224-1 "Privacy Act Notification (July 1996),

Federal Acquisition Regulations (FAR) Clauses pertaining to the Privacy Act and are included in the contract.

☐ 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.

☒ No

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

☒ Yes.

OSFCP generates an access log file which captures the following information:

- The username and email address of both managed and external users
- IP address of the end user that is making a request to access the application and its resources
- Date timestamp
- Successful and unsuccessful login attempts
- The file path and filename(s) of resources accessed during the user's session
- Content accessed or opened
- File size of uploaded content
- Removed collaborator(s)
- Administrative changes to the application (administrator-only)
- New users created or removed users (administrator-only)

*Important Note: Only the application administrator or co-administrator has privileged access to the OSFCP administrative console which produces such logs and reports.

☐ No

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

A report is generated on user activity which includes username, email address, account status, IP address of the end user that is making a request to access the application and its resources, date timestamp, successful and unsuccessful login attempts, the file path and filename(s) of resources accessed during the user's session, content accessed or opened, and the file size of uploaded content.

**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.

The cloud service provider is responsible for the implementation of all physical security controls.

(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. Mobile Authenticator Application

Certain technical controls such as firewall, user identification, IDS, VPN, and PIV are implemented in a hybrid manner by both Box and the 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.

(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.

**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 Director of Information Technology Division who is the OSFCP system owner and Senior OIG leadership, the OI Assistant Special Agent in Charge (ASAC), Director of Information Security, and the authorizing official are responsible for oversight and management of the security controls and the protection of agency information processed and stored in OSFCP. 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 OSFCP, and coordinating Privacy Act requests for notification, access, amendment, and complaints with the Privacy Act System Manager 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?**

From a cloud customer perspective, the OI ASAC, Director of Information Security, and the authorizing official are responsible for daily operational oversight and management of the system's security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. Both the OSFCP Information System Owner and Information System Security Officer are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC, DOI's incident reporting portal, within 1-hour of discovery in accordance with Federal policy and established DOI procedures, and that appropriate remedial activities are taken to mitigate any impact to individuals in

coordination with OIG and DOI Privacy Officials.

As CSPs, Box and AWS are responsible for establishing and implementing a reliable incident response process for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information. This process will be initiated when it is proven that such events were not caused by any misconfigured application settings or any other access control-related negligence by the OIG. The CSP is required to immediately report any potential breach of PII to OIG.