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: Computer Crimes Unit Network-General Support System (CCUNet-GSS)
Bureau/Office: Office of Inspector General (OIG) / Office of Investigations (OI)
Date: January 23, 2023
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:

B. What is the purpose of the system?

The purpose of the system is to facilitate the OIG's various responsibilities under the Inspector General Act of 1978, as amended, to conduct and supervise investigations relating to programs and operations of the Department of the Interior (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.

CCUNet-GSS is a small, segregated local area network (LAN) of storage servers and a series of standalone laptops and desktop towers with no system interconnection to any other DOI network or OIG General Support System (OIG-GSS). The CCUNet-GSS consists of a suite of forensic software tools, such as Axiom Magnet, Encase, and Forensic Toolkit (FTK) which support a team of forensic agents who obtain, examine, and analyze various forms of digital evidence from government-issued devices such as laptops, iPads, and iPhones, as well as, documents such as PDFs, Word documents, Excel spreadsheets, and electronic mail (email).

The CCUNet-GSS provides a standalone network environment where digital forensic evidence can be collected, analyzed, and stored to support ongoing OIG investigations involving computer crimes. In some cases, digital evidence may include contraband such as unsuitable or disturbing images as well as malware. The individuals who are subject to the investigation that are included in the case files may be employees from OIG, DOI bureaus and offices, as well as other individuals external to the agency. In addition, all digital evidence is required to be protected from unauthorized access and tampering so that such evidence can be admissible in court. For these reasons, CCUNet-GSS is separated from the OIG-GSS and other DOI networks.

There are six network-area-storage (NAS) servers and roughly 20 forensic laptops – all standalone endpoints. When digital forensic evidence is received, the original file is hashed and stored on the NAS servers, while a copy is created for examination and analysis purposes and is stored on individual forensic laptops.

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:

CCUNet-GSS was added to the DOI Governance, Risk and Compliance platform.

☐ 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).

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:

☒ 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 found in 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, financial business information, 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 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 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.

CCU staff are required to provide their username and password to create an account to access the system.

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.

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, reports generated from DOI OIG's Case Management System (CMS) and Nuix, emails from Microsoft Office 365 or eMail Enterprise Records Document Management System (eERDMS) and voluntary disclosures from individuals.

CMS is 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.

Nuix is a web-based, commercial-off-the-shelf (COTS) product used by OI within the OIG that makes evidence data securely and conveniently available to its users.

Microsoft Office 0365 is a service product of Microsoft that enables common Enterprise Architecture through a flexible and convenient cloud offering. Bundling of Office 365 services allows DOI to simplify administration of licenses and subscriptions to services at an enterprise level, and facilitates system-wide user management, password administration, and oversight of security controls.

eERDMS is a major application that helps DOI meet its objective to identify, acquire and deploy an enterprise application that combines electronic workflow, imaging, and management of documents, e-mails, discovery, and records. eERDMS provides the framework for enterprise use for storing, accessing, and managing the DOI's records, regardless of format, media, source or location.

Please see the OIG-GSS, eERDMS, and Microsoft O365 PIAs for more information. These PIAs may be viewed on the DOI PIA website at https://www.doi.gov/privacy/pia.

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:

Access to information is restricted to those authorized and holding appropriate security clearances. Particularly, access to the CCUNet-GSS is strictly limited to OIG CCU forensic staff. PII within this system may be shared with authorized personnel within the OIG as part of the investigative or report development process.

☒ 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, as amended. 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 SORN, INTERIOR/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 SORN, INTERIOR/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).

☐ Contractor:

☒ Other Third Party Sources:

PII may be shared in reports prepared for Congress or may be included in published reports for the public as authorized and necessary to support the mission of the OIG.

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 email, DOI owned electronic assets, network or information systems, and for audio and visual recordings, individuals who enter on DOI 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 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:

Individuals are advised of their rights on the Complaint Hotline page which includes an Information Disclosure and Privacy Act Notice. Due to the purpose and nature of the system and

to help facilitate the OIG's law enforcement investigations, generally individuals are not provided with a Privacy Act notice or have the opportunity to consent to the collection or use of their information. Law enforcement records are exempt under 5 U.S.C. 552a(j)(2) and (k)(2).

☒ Privacy Notice:

Notice is provided through the publication of this privacy impact assessment and the publication of the INTERIOR/OIG-2, Investigative Records SORN referenced above 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).

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 OIG information systems 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 is retrieved by manually entering keywords relevant to the nature of the case. Identifiers may include subject names, addresses, phone numbers, email addresses, or any other identifiers contained within the forensic evidence. Data can also be automatically filtered by date/time, file type, or other file metadata non-specific to an individual.

I. Will reports be produced on individuals?

☒ Yes:

Software programs within the CCUNet-GSS are capable of ingesting forensic information and generating case documentation. For example, Axiom Magnet – a program or tool installed on CCUNet-GSS laptops - has report generation capabilities. However, this information is limited to any investigative evidence which is uploaded, tagged, and accessible by an individual CCU end user who is working on a case. Reports may include names and other identifying

information related to case files and investigations. Only authorized OIG officials have access to the reports.

☐ No

Section 3. Attributes of System Data

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

The forensic data reviewed within the CCUNet-GSS will be "hashed" by the OIG 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 independent corroborate or verify the accuracy of data collected per OIG policy and procedures. Supervisors will also review data for accuracy. Information is not collected directly from individuals. Information collected from OIG agents during an investigation is provided to CCU staff to enter into the CCUNet-GSS.

B. How will data be checked for completeness?

CCU agents and OIG analysts 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).

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 as well as internal DOI OIG information systems and various investigative processes that are designed to determine or verify the information.

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

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

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 fiscal year.

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, and other internal DOI bureau investigation activities. 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 and privacy controls 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.

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 SORN described in Section 1, Question G above provides constructive notice. Note that DOI claimed Privacy Act exemptions for records maintained under INTERIOR/OIG-2, Investigative Records, 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 SORN 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 – There is a risk that the system may collect, store or share more information than necessary. The PII collected and used in the system is limited to what is necessary to perform the investigative functions and support the OIG's mission to prevent fraud, waste and abuse. PII is used for its intended purpose in support of the OIG mission. Data within the system is protected by the security controls provided by the CCUNet-GSS. The processing of forensic data in the CCUNet-GSS takes place internally within its related forensic software. 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.
- Retention – There is a risk that information will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. CCUNet-GSS maintains all records with PII in accordance with applicable records retention or disposition schedules approved by NARA or based on the need and relevancy of the data in the support of the OIG mission. Some records are maintained as permanent records due to their Continuing Historical Value, all other temporary records are disposed of in accordance with approved records schedules.
- Processing – There is a risk related to processing of PII during investigations. This risk is mitigated by restricting access to a limited number of authorized OIG forensic examiners. Processing is performed by OIG CCU staff in a closed, alarmed, access-controlled lab on a stand-alone forensic computer workstation with appropriate security controls including encryption for data at rest and data in transit.
- 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 organizations only for authorized purposes. The authorized sharing of information in support of law enforcement activities is described in the routine uses published in the INTERIOR/OIG-2, Investigative Records SORN. Memorandums of Agreements are in place for any sharing with external organizations.
- 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.

CCUNet-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:

The use of PII within CCUNet-GSS 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:

CCUNet-GSS 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 be 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 CCUNet-GSS 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 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/sorn. Law enforcement records are exempt under 5 U.S.C. 552a(j)(2) and (k)(2).

☐ No

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

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.

As referenced earlier in Section 2.C., data is derived and consolidated from other internal applications and external systems. Unauthorized access to data contained in the system is protected through the controls of the CCUNet-GSS by:

- Standalone, non-interconnected system
- Only authorized personnel with proper credentials/background investigation can access the system
- Least privilege access
- Role-based access control
- Username and password
- Each forensic Dell laptop has BitLocker enabled for data-at-rest encryption
- Original forensic data is stored on standalone network servers

☒ Yes, processes are being consolidated.

Depending on the circumstance of an investigation, forensic files may be admissible in court. To maintain data integrity and proper chain of custody of forensic data, the current process is to make a copy of the original file(s) which serves as the "working copy" by CCU forensic examiners for the investigative and analytical purposes. For protection, the "working copy" is saved on CCU forensic laptops which have BitLocker enabled for data-at-rest encryption. Meanwhile, original forensic file(s) remains securely stored on standalone network servers.

☐ 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:

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 roles and 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.

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.

☒ 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.

The system is not intended to locate and monitor individuals except to the extent needed to support OIG investigations. CCUNet-GSS forensic laptops require the CCU agents to identify and authenticate themselves by providing their respective username and password. User activity is captured or monitored via user logs and to an extent, event logs.

☐ No

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

The kinds of information collected includes username of the CCU end user, the file path and filename(s) of content accessed or opened, date and time stamp, and the file size of stored content. This informationcan be retrieved from network storage servers and laptops

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 CCUNet-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.

This system is not connected to the internet. OIG CCU staff must physically be present to access the closed, alarmed, access-controlled lab.

(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.

This system is not connected to the internet. OIG CCU staff must physically be present to access the closed, alarmed, access-controlled lab.

(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 Assistant Special Agent in Charge (ASAC) within the CCU serves as the CCUNet-GSS Information System Owner and the official responsible for oversight and management of the security controls and the protection of agency information processed and stored in CCUNet-

GSS. In coordination with the OIG Associate Privacy Officer, the Information 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 CCUNet-GSS, 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?

The ASAC with the CCU, 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. The CCUNet-GSS 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.