PRIVACY IMPACT ASSESSMENT

Effective Date: June 26, 2026

DOL Office of Inspector General (DOL-OIG) Labor Office of Inspector General Case Activity Tracking System (LOCATS)

☒Concurrence of Senior Agency Official for Privacy

☐Non-concurrence of Senior Agency Official for Privacy

Braye Cloud, Senior Agency Official for Privacy (SAOP)
Deputy Assistant Secretary for Operations
Office of the Assistant Secretary for Administration & Management

OVERVIEW & GENERAL INFORMATION

As required by the E-Government Act of 2002 (as amended) and OMB Memorandum M-03-22, OIG has developed this Privacy Impact Assessment to describe:

1. The information to be collected with a particular focus on personally identifiable information (PII);
2. Why the information is being collected including the legal authority for the information collection;
3. The intended use of the information;
4. With whom the information will be shared (such as internal uses with other DOL component agencies or another federal agency);
5. What notice is provided to individuals, what opportunities are given to individuals to consent to particular uses of the information, how individuals can grant consent, and what opportunities individuals have to decline to provide information;
6. How the information will be secured with administrative and technological security controls;
7. Whether a *system of records* is being created under the Privacy Act, 5 U.S.C. 552a; and
8. The analysis of privacy risk associated with the collection, use, storage, and dissemination of information and practices that have an impact on privacy.

Name of System (and Acronym, if applicable)

Labor Office of Inspector General Case Activity Tracking System (LOCATS)

Location of the System

LOCATS is built on AINS (dba) by Opexus, an eCase Case Management System, Software as a Service (SaaS). Opexus manages the LOCATS platform in their Ashburn VA facility. The Office of Inspector General (OIG) documents are stored in the eCase SharePoint repository.
The OIG's Office of Labor Racketeering and Fraud Investigations (OLRFI) personnel, and Branch of Database Management and Applications (BDMA) support personnel, will access LOCATS using a dedicated VPN from the OIG GSS, which is connected through the Department of Labor through a 100-MB fiber optic connection. The connection is used to allow OIG users access LOCATS. All OIG personnel will use Government provided equipment, authenticated by the OIG Active Directory use GSS networks over the dedicated VPN to the AINS (dba) Opexus facility. All access is monitored and controlled by Palo Alto Fireboxes.

Brief Description of the System

LOCATS is a major application system dedicated to the mission of the OIG's Office of Labor Racketeering and Fraud Investigations (OLRFI). The system is designed to help OLRFI conduct criminal investigations related to labor racketeering and organized crimes in the nation's labor unions. The application will store, track, retrieve, and report electronic investigative data produced during the investigative process.

Purpose of the System:

☒ Program administration	☐ Employee or customer satisfaction surveys
☐ Computer Matching Program	
☐ Administering human resources programs for DOL or federal government personnel	☐ Improve Federal services online
☒ Litigation	☒ Promote information sharing initiatives
☒ Criminal law enforcement activities	☒ Civil law enforcement activities
	☐ Other

This System is operated by:

☒ Component agency: Office Inspector General, Office of Investigations (OI) and Office of Special Investigations (OSI)

☒ Contractor (4 Contractors -OIG cleared Cloud Service Provider Opexus contractors)

For a system operated by a contractor, the contract or other acquisition-related documents includes privacy requirements:

☒ Yes
☐ No

This PIA is being conducted for:

☐ A new information system or project that collects, maintains, or disseminates information in identifiable form.

☐ A new collection of information subject to the Paperwork Reduction Act because it is for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government in the scope of their employment).

☐ A change to the PII Confidentiality Impact Level (NIST SP 800-122) or System Security Categorization (NIST SP 800-60).

☒ An existing system subject to a periodic review at the 5-year mark.

☐ An existing system with significant changes that create new privacy risks.

The following are the significant changes that create new privacy risks:

☐ Changed information collection authorities.

☐ Changed business processes.

☐ Conversion of paper-based records to electronic systems.

☐ Anonymous to Non-Anonymous. This is when functions applied to an existing system change anonymous information into information in identifiable form.

☐ Significant System Management Changes. This is when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system.

☐ Significant Merging. This is when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated.

☐ New Public Access. This is when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public.

☐ Commercial Sources. This is when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources.

☐ New Interagency Uses. This is when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form.

☐ Internal Flow or Collection. This is when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form.

☐ Alteration in Character of Data. This is when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information).

☐ Other

The class(es) of users who will have access to the system are:

☐ General Public
☒ Contractors
☒ Government Employees
☐ Other

1. INFORMATION IN THE SYSTEM

OIG -OI collects certain types of information from certain sources using particular methods to collect the information, as identified below.

1.1. The information that is collected, used, maintained, or disseminated in connection with the system is:

☒ Name/Former Name	☒ Date of Birth	☒ Maiden Name	☒ Place of Birth	☒ Citizenship
☒ Social Security number (including in truncated form)	☒ Driver's License	☒ Financial Account	☒ Taxpayer ID	☒ Passport Number
☒ Sex	☒ Telephone Number	☐ Criminal Record	☐ Education	☒ Age
☒ Financial Transaction	☒ Employer ID	☒ Alien Registration Number	☒ Vehicle Identifier	☒ Employee ID
☒ Credit Card	☒ Medical Record	☒ File/Case ID	☒ Financial Information	☐ Religion
☒ Alias	☒ Home Address	☒ Military Service	☒ Mother's Maiden Name	☒ Medical Information
☒ Email Address	☐ Marital Status	☒ Race/Ethnicity	☒ Occupation	☒ Work Email Address
☒ Job Title	☐ Salary	☒ Business Associates	☒ Work Telephone Number	☒ Proprietary or Business Information
☐ Employment Performance Ratings	☒ Work Address	☐ Work History	☒ Procurement or contracting records	☐ Other Performance Information
☒ Fingerprints	☒ Scars, Marks, Tattoos	☒ Signatures	☒ Photographs	☐ Palm Prints
☒ Hair Color	☐ Vascular Scans	☒ Weight	☒ Voice/Audio Recording	☒ Eye Color
☐ DNA Sample or Profile	☐ Dental Profile	☒ Video Recording	☒ Height	☐ Retina/Iris Scans
☒ User ID	☒ IP Address	☐ Other PII		

1.2. The information is collected using the following methods:

☒ Website-based forms
☒ Paper forms

☒ Electronic forms
☒ Verbal collection
☒ No form - the information collected does not require a specific form

1.3. The source of the information is:

Directly from the Individual about Whom the Information Pertains		
☒ In Person	☒ Hard Copy: Mail/Fax	☒ Web-based (uploading through an app or website)
☒ Telephone	☒ Email	☒ Legal or other representative: Attorney and Court interactions such as charging documents, court orders etc.
☐ Other		

Government Sources		
☒ Within the Component Agency	☒ Other DOL component agencies	☒ Other Federal Agencies
☒ State, Local, Tribal	☒ Foreign	☐ Other

Non-government Sources		
☒ Public Organizations	☒ Private Sector	☒ Commercial Data Brokers
☒ Third Party Website or Application	☒ Other: Employer	

1.4. Social Security numbers (SSN) are collected:

The Privacy Act of 1974 requires that when DOL requests that an individual provide a Social Security number, DOL must indicate whether that disclosure is mandatory or voluntary and by what statutory or other authority the number is being requested including what uses will be made of it.

Additionally, OMB Circular A-130 to the Heads of Executive Departments and Agencies regarding *Managing Information as a Strategic Resource* includes a requirement that DOL take steps to eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to the use of Social Security numbers as a personal identifier.

Finally, DOL policies permit component agency programs to collect, use, maintain, and disseminate SSNs only when required by law (e.g., statute, Executive Order, or upon approval of the SAOP or SAOP designee).

Will SSNs be collected for this system, whether directly or indirectly from the individual to whom the SSN applies?

☐ No

☒ Yes

1.4.1. If yes, the specific authority relied upon to collect SSNs?

Section 6(a)(1) of the Inspector General Act of 1978, (Pub. L. 95-452, § 1, Oct. 12, 1978, 92 Stat. 1101), authorizes The Inspector General to "have access to all records, reports, audits, reviews, documents, papers, recommendations, or other material available to the applicable establishment which relates to programs and operations with respect to which that Inspector General has responsibilities.

1.4.2. The purpose for the collection of SSNs and how the SSN will be used is as follows:

SSNs are being collected for the purpose of law enforcement investigations.

1.4.3. The following alternatives were considered in lieu of the collection of SSNs:

No alternative was considered because OI uses SSNs to verify identities of individuals whose identities may otherwise be mistaken with other individuals with the same name.

1.4.4. The alternatives were not selected because:

No alternative was considered.

1.5. The information collected is subject to the Paperwork Reduction Act:

☐ Yes, some or all of the information is covered by the Paperwork Reduction Act.

- ☐ The information expected to be collected does not yet have an OMB control number but will be submitted for PRA approval.
- ☐ The information collected is part of an existing collection and the OMB control number for the collection is

☒ No, the information collected is not subject to the Paperwork Reduction Act.

2. WHY THE INFORMATION IS BEING COLLECTED

2.1. Why is the information being collected?

The information is being collected for law enforcement investigations and other purposes.

2.2. The following are the specific legal authorities and/or agreements that permit the collection, use, maintenance, and/or dissemination of information (including any PII) by the system:

The Inspector General Act of 1978, (Pub. L. 95-452, § 1, Oct. 12, 1978, 92 Stat. 1101), as amended by Section 812 of the Homeland Security Act of 2002 (Pub. L. No. 107-296), authorizes the Inspector General to conduct audits and investigations that relate to the OIG's mission.

3. INTENDED USE OF THE INFORMATION

3.1. The information collected by the system is used in the following ways:

The information collected by the system is used for law enforcement investigations.

3.2. The system aggregates or analyzes information to create new information:

☐ Yes
☒ No

4. INFORMATION SHARING AND ACCESS

4.1. Will OIG - OI share data internally or externally?

☒ Yes, the PII in the system will be shared.
☐ No, The PII in the system will not be shared.

Internal Sharing:

Component Agency	Information Shared	Purpose
Office of Audit	Summary information.	For agency's mission.

External Sharing:

Organization	Information Shared	Purpose	MOU or other Agreement
International Organized Crime Intelligence and Operations Center (IOC-2)	Indexes and case summary information	Case deconfliction	Memorandum of Understanding (MOU) and Interagency Service Agreement (ISA)
US Attorney's Office	Any information that is relevant to the prosecution of the case.	Prosecution	Per U.S. Code; Department of Justice, Justice Manual

Law Enforcement Agencies	Investigative findings	Joint Force Investigations	MOUs or other agreements are not required for joint investigations.

4.2. Does OIG-OI place a limitation on re-dissemination of PII shared with internal or external organizations?

Internal Sharing

☒ Yes, another DOL component agency is required to verify with the component agency operating the system before re-dissemination of PII.
The Office of Audit is required to verify with The Office of Investigations, who operates the system, before re-dissemination of PII.

☐ No, another DOL component agency is not required to verify with the component agency operating the system before re-dissemination of PII.

☐ Not applicable, the component agency does not share PII with other DOL component agencies.

External Sharing

☒ Yes, the external agency or entity is required to verify with the DOL component agency before re-dissemination of PII.
The International Organized Crime, Intelligence and Operations Center (IOC-2) is required to verify with The Office of Investigations, who operates the system, before re-dissemination of PII.

☐ No, the external agency or entity is not required to verify with the DOL component agency before re-dissemination of PII.

☐ Not applicable, the component agency does not share PII with external agencies or entities.

4.3. Indicate whether the system connects with or receives information from any other systems authorized to process PII.

☐ Yes, this system connects with or receives information from another system(s) authorized to process PII.

If the answer to 4.3 is yes, provide the name of the system and describe the technical controls which prevent improper accessing of the PII while in transit.

☒ No, this system does not connect with or receive information from another system(s) authorized to process PII and/or BII.

5. NOTICE, CONSENT, AND OPPORTUNITY TO DECLINE TO PROVIDE INFORMATION

5.1. Indicate whether individuals will be notified if their PII is collected, maintained, or disseminated by the system.

☐ Notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.
☐ Notice is provided by a Privacy Act Statement and/or a Privacy Notice. The Privacy Act Statement and/or Privacy Notice can be found on the following forms or information collection instruments:
☐ Notice is provided by other means.
☒ Notice is provided by means of this Privacy Impact Assessment.
Note: Notice is not provided to those individuals who are under active investigations.

5.2. Do individuals have an opportunity to decline to provide PII?

☐ Yes, individuals have an opportunity to decline to provide PII.
☒ No, individuals do not have an opportunity to decline to provide PII.
PII is required to ensure the accuracy of the individual being investigated. However, in cases involving complaints, individuals may choose to not provide PII by submitting the complaint anonymously.

5.3. Do individuals have an opportunity to consent to particular uses of their PII?

☐ Yes, individuals have an opportunity to consent to particular uses of their PII.
☒ No, individuals do not have an opportunity to consent to particular uses of their PII.
Individuals do not have an opportunity to consent to particular uses of their PII because of case related investigations.

5.4. Do individuals have an opportunity to review or update PII pertaining to them?

☐ Yes, individuals have an opportunity to review or update PII pertaining to them.
☒ No, individuals do not have an opportunity to review or update PII pertaining to them.
Individuals under investigation do not have the opportunity to review or update PII pertaining to them after it is submitted.

6. HOW INFORMATION IS SECURED

As required by the E-Government Act of 2002 and OMB Memorandum M-03-22, DOL imposes certain administrative and technological controls on each system that contains PII. Below, DOL describes whether it has conducted a risk assessment, the security controls to put in place to protect against that risk, and how those controls are implemented. DOL also describes how it continuously monitors the system to ensure that the controls continue to work properly, safeguarding the information. Individuals who have questions regarding the information below may reach out to DOL's Privacy Program at privacy@dol.gov.

6.1. Administrative controls for the system:

☒ PII is kept in a secured physical location.
Server is located in GOV CLOUD FISMA high facility where physical control is implemented by the Opexus cloud service provider.

☐ All users signed a confidentiality agreement or non-disclosure agreement.

☒ All users are subject to a Code of Conduct that includes the requirement for confidentiality.
All users are subject to the Rules of Behavior.

☒ DOL Personnel (employees, contractors, interns, volunteers) receive **annual** training on privacy and confidentiality policies and practices.
All users must take the annual Rules of Behavior training and the Cybersecurity and Privacy Awareness Training (CSPA) via LearningLink.

☐ DOL Personnel receive **role-based** training on privacy and confidentiality policies and practices. ☐ DOL Personnel (employees, contractors, interns, volunteers) receive **system-specific** training on privacy and confidentiality policies and practices.

☒ Access to the PII is restricted to authorized personnel only.
Access to PII is restricted to authorized users only based on user roles, functions and assigned privileges in the system.

☐ Appropriate NIST SP 800-53 Revision 4 security controls for protecting PII are imposed.

- ☐ A security assessment report has been prepared for the information system to identify all privacy risks for continuous monitoring.

☒ Appropriate NIST SP 800-53 Revision 5 security controls for protecting PII are imposed.
The controls will be imposed through continuous monitoring using NIST Risk Management Framework through annual security assessment.

- ☒ A security assessment report has been prepared for the information system to identify all privacy risks for continuous monitoring.
  The last SAR date for LOCATS was completed October 9, 2024. LOCATS undergoes continuous monitoring annually where one third of its security controls and privacy controls are assessed. For FY24 a total of 39 controls were assessed with 29 controls as satisfied and 10 controls other than satisfied.

☒ There is one or more Plan of Action and Milestones (POA&M) associated with this system.
LOCATS as of 6/16/2026 has four (3) open POA&Ms related to Multifactor Authentication (MFA) on the application level, RA-8, Privacy Impact Assessment, and SC-07(24) Personally Identifiable Information. The completion of this PIA will resolve two of the existing POA&Ms for LOCATS.

☒ Contractors that have access to the system are subject to information security provisions in their contracts required by DOL policy.
All contractors are subject to an OIG specific Pre-Employment Clearance Inquiries (PECI) process and approval.
☒ Contracts with customers establish DOL ownership rights over data including PII.
All contractors are subject to an OIG specific Pre-Employment Clearance Inquiries (PECI) process (PECI is OIGs pre-employment background investigation) and approval before access to the system.
☐ Other:

6.2. Technological controls for the system:

☒ Access to the PII is being monitored, tracked, or recorded:
OIG Firewall monitors and prevents unauthorized users. Access is monitored and recorded by user access logs. Audit logs from the system are pulled by the Information Security Office on a monthly basis and stored on a SharePoint.
☒ User Log In Credentials
Identification is used for system access, such as username/password/PIV card. Both DOL personnel and non-DOL users are authenticated through the network and then the application.
☒ Virtual Private Network (VPN)
Access is limited to OIGs networks through VPN currently using Zscaler.
☐ Biometrics
☒ Encryption of Data at Rest
Encryption of Data at Rest is an inherited control implemented by Opexus, cloud service provider.
☒ Firewall
OIG Firewall monitors and prevents unauthorized users from accessing OIG's internal network from the internet.
☒ Role-based Access Controls
LOCATS admins assign the access level to all users based on their roles. System users and the associated attributes will be synchronized with LOCATS. As part of this synchronization, users will be assigned into defined groups, which can include privileged and non-privileged roles. This user group will determine the level of access and actions users can take within LOCATS eCase application.
☒ Encryption of Data in Transit
Data in Transit is an inherited control implemented by the Opexus Cloud Service Provider (CSP). All data transmitted are encrypted by the CSP.
☒ Use Only for Privileged (Elevated Roles)
LOCATS admins assign the access level to all users based on their roles. This is a privileged role within LOCATS. Admins can also assign privileged roles to users.
☐ Other:

6.3. Retention of Information

Information in the system is covered by an approved records retention schedule and monitored for compliance.

☒ Yes.
LOCATS records are maintained for fifteen (15) years for Racketeering cases and fifteen (15) years for fraud cases with the General Records Schedule as follows N9-174-9902-02, Labor Racketeering Investigative Case Files, N1-174-002-2 Analysis, Compliant and Evaluation (ACE) Files, N9-174-93-1, OLR Investigation Case Files and Zero files, NC1-174-93-1, OLR Investigation Case Files and Zero Case Files Maintained by OLR Headquarters, N1-174-00-1, OIG Investigative Case Files.
☐ No.
☐ A records retention schedule is in development.

If there is an approved record retention schedule, is retention monitored for compliance to the schedule?

☒ Yes, retention is monitored for compliance to the schedule.
☐ No, retention is not monitored for compliance to the schedule.
☐ No, there is not an approved record retention schedule.

When information is no longer needed, it is disposed of by:

☐ Shredding or other physical destruction
☐ Overwriting
☐ Physical destruction of hardware, such as degaussing
☐ Deleting
☒ Other: In accordance with the investigative case file NARA records schedule. We follow NARA disposition schedule depending on the document type. Disposal method can vary depending on the type of case and evidence at issue.

7. SYSTEM OF RECORDS NOTICE (SORN)

The Privacy Act of 1974 (Privacy Act) requires DOL to permit individuals to gain access to their records (including obtaining copies and requesting amendments to the records) and any information pertaining to the requesting individual which is contained in a "system of records" (a specifically defined term under the Privacy Act). Although many DOL Information Systems may contain PII, they are not all required to have a SORN. For purposes of the Privacy Act, a system of records that requires a SORN refers to any group of any records under the control of DOL (including through a contractor) from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Some systems of records under DOL's control may be exempt from some of the Privacy Act rights provided to individuals. DOL is identifying all of the SORNs applicable to this system so that individuals may review the SORNs for more detailed additional information.

7.1. This system is covered by one or more existing SORNs.

DOL/OIG-11 Investigative Case Files and Tracking System, Case Development and Intelligence Records, USDOL/OIG

7.2. This system:

☒ Does not require an additional SORN beyond those identified above.
☐ Does not require a SORN.
☐ Requires a new or additional SORN.
☐ Requires a modification to the following SORN(s):

Reason for Modifying SORN(s):

☐ A significant increase in the number, type, or category of individuals about whom records are maintained.
☐ A change that expands the types or categories of information maintained.
☐ A change that expands the types or categories of information maintained.
☐ A change that modifies the scope of the system.
☐ A change that modifies the purpose(s) for which the information in the System of Records is maintained.
☐ A change in the agency's authority to maintain the system, collect, use, or disseminate the records in the system.
☐ A change that modifies the way in which the system operates or its location(s) in such a manner as to modify the process by which individuals can exercise their rights under the statute.
☐ A change to equipment configuration (either hardware or software), storage protocol, type of media, or agency procedures that expands the availability of, and thereby creates substantially greater access to, the information in the system.
☐ The addition or rescindment of a Privacy Act exemption.
☐ A new routine use or significant change to an existing routine uses that has the effect of expanding the availability of the information in the system.

8. ANALYSIS OF PRIVACY RISK

8.1. PII Confidentiality Impact Level from NIST Special Publication 800-122

Indicate the potential impact/harm that could result to the subject individuals and/or DOL if PII were inappropriately accessed, used, or disclosed.

☐ **Low** – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

☒ **Moderate** – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
☐ **High** – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals

8.2. Identification and evaluation of potential risks to privacy

Adequacy of Privacy Training for DOL personnel

ALL OIG users and contractors must take the annual Cybersecurity and Privacy Awareness training (CSPA) and Rules of Behavior Training in LearningLink.

How Information is Acquired, Stored, and Shared

LOCATS information is acquired through various law enforcement techniques, such as subpoena's, interviews and surveillance. The data is encrypted in transit and at rest; stored in a GOV cloud high facility with the cloud service provider (CSP) Opexus and is accessible to OIG law enforcement personnel only. A subset of the data is shared with IOC2 and relevant data shared with the US attorney's office. As data is shared internally and externally, it poses a risk of PII unintentionally being exposed by the receiving party, incorrect information such as the wrong request containing PII can be sent, the correct request containing PII can be sent to the wrong agency or US attorney. Sharing information electronically also carries a risk by adversaries that would attempt to gain access to our information systems.

Describe the choices that were made with regard to preventing or mitigating these privacy risks

The data contained in LOCATS is encrypted in transit and at rest; stored in a GOV cloud high facility with the cloud service provider (CSP) Opexus and is accessible to OIG law enforcement personnel only. We rely on the office of investigations personnel to follow PII safeguarding best practices which are standard throughout the Federal government. Information is encrypted and password protected when appropriate.

Protection against PII Breaches

Unauthorized Data Access:

Sharing information carries a risk by adversaries who may attempt to gain access to the data on the system. A firewall monitors and prevents unauthorized users from accessing OIG's internal network from the Internet. There are no public access accounts. All access is monitored and controlled by firewalls Additional monitoring of access from the Internet is provided by Internet Service Provider sensors.

Potential Misuse of Data:

Users who already have access to the system carries the risk of potential misuse of data. LOCATS assigns specific access rights to users depending on their roles and need to know limiting PII exposure. All access is monitored and controlled by a Firewall. Audit logs from the system are pulled by the Information Security Office on a monthly basis.

Protecting Against Insider Threats:

Insider threats are assessed to be minimal. Any potential exposure is primarily associated with administrative errors. In addition, user audit logs are also reviewed monthly basis to identify any anomalies or unauthorized activities.

Describe the choices that were made with regard to preventing or mitigating these privacy risks

Unauthorized Data Access: OIG has Firewalls in place that monitors and prevents unauthorized users from accessing OIG's internal network from the Internet. There are no public or temporary access accounts for LOCATS. All access is monitored and controlled by firewalls. Access requires multifactor authentication (MFA) to access system. Users are granted least privileges access for the performance of their roles and casefiles they are working on.
Potential Misuse of Data: LOCATS has access and permission roles that prevent those without a need to know from accessing casefiles. OIG places a limitation on the information shared internally or externally whereby DOL component agency is required to verify with the component agency operating the system before re-dissemination of PII or data.
Protecting Against Insider Threat: All users have an official need to know associated with the user roles and investigative cases they are working on. User audit logs are also reviewed monthly to detect any anomaly or unauthorized activities.

Other:

N/A

Describe the choices that were made with regard to preventing or mitigating these privacy risks

N/A

Appendix 1. Artificial Intelligence (AI) and Machine Learning (ML)

To be completed by an information system that integrates an AI/ML component

Name the AI and or ML application?

Describe what the AI/ML is being used for?

Does the AI/ML component input, access, process, store, analyze, or generate outputs using any PII?

☐ Yes

X No

If yes, what PII elements are accessed, processed, or generated by the AI/ML component?

☐ Name/Former Name	☐ Date of Birth	☐ Maiden Name	☐ Place of Birth	☐ Citizenship
☐ Social Security number (including in truncated form)	☐ Driver's License	☐ Financial Account	☐ Taxpayer ID	☐ Passport Number
☐ Sex	☐ Telephone Number	☐ Criminal Record	☐ Education	☐ Age
☐ Financial Transaction	☐ Employer ID	☐ Alien Registration Number	☐ Vehicle Identifier	☐ Employee ID
☐ Credit Card	☐ Medical Record	☐ File/Case ID	☐ Financial Information	☐ Religion
☐ Alias	☐ Home Address	☐ Military Service	☐ Mother's Maiden Name	☐ Medical Information
☐ Email Address	☐ Marital Status	☐ Race/Ethnicity	☐ Occupation	☐ Work Email Address
☐ Job Title	☐ Salary	☐ Business Associates	☐ Work Telephone Number	☐ Proprietary or Business Information
☐ Employment Performance Ratings	☐ Work Address	☐ Work History	☐ Procurement or contracting records	☐ Other Performance Information
☐ Fingerprints	☐ Scars, Marks, Tattoos	☐ Signatures	☐ Photographs	☐ Palm Prints
☐ Hair Color	☐ Vascular Scans	☐ Weight	☐ Voice/Audio Recording	☐ Eye Color

☐ DNA Sample or Profile	☐ Dental Profile	☐ Video Recording	☐ Height	☐ Retina/Iris Scans
☐ User ID	☐ IP Address			
			☐ Other PII	

Does the AI component transmit/maintain PII to any external systems, vendors, or cloud services?

How is PII protected when used by the AI/ML component?

APPROVAL SIGNATURE PAGE

Reviewed by: Scott Ewalt, OIG Administrative Officer (AO)

SCOTT EWALT Digitally signed by SCOTT EWALT
Date: 2026.06.30 12:47:08 -04'00'

Signature

THE FOLLOWING OFFICIALS HAVE REVIEWED THIS DOCUMENT

Reviewed by: Efua Colecraft, Information System Security Officer (ISSO)-OIG ☒

Reviewed by: Todd Bailey, Chief Information Officer, OIG ☒

Reviewed by: Lisa Finnican, OIG Attorney Advisor ☒

Reviewed by: Muhammad Butt, Emerging Technology and Senior Advisor for Cybersecurity Initiatives OASAM-OCIO ☒

Reviewed by: Mara Blumenthal, DOL Privacy Office Branch Chief OASAM-OCIO ☒