United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official.
All entries must be Times New Roman, 12pt, and start on the next line.
If you need further assistance, contact your LPO. A listing of the LPOs can be found here:
https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

System Name: WingSwept (WS)	**System Owner: James Conrad**
Preparer: Alexander Stone	**Office: Office of Inspector General (OIG)**
Date: 10/1/2024	**Phone: 202-815-9867**
Reason for Submittal: New PIA__X__ Revised PIA____ Annual Review____ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☐	
Operation & Maintenance ☒ Rescindment/Decommissioned ☐ **Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).** **The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).**	

Provide a general description/overview and purpose of the system:

WingSwept Case Management and Tracking System (CMTS), (also referenced as OIG-WS in Xacta) is an investigative case management and tracking system being implemented by OIG to replace the following functions currently handled via the Inspector General Enterprise Management System (IGEMS): IGEMS Investigative Module (I2M), Hotline Requests and Forms, and Office of Special Review and Evaluation (OSRE) Administrative Investigation Directorate (AID) investigation files.

All data within IGEMS has been imported into WingSwept. IGEMS will maintain archival case data processed prior to July 2024 for records retention purpose. The system owner will dispose of records in

IGEMS according to the records retention schedule. The IGEMS system will be fully decommissioned once all the archival records have met the full life cycle of the data according to the records retention schedule.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

Inspector General Act of 1978, 5 U.S.C. as amended

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

Yes. It is updated and reviewed yearly. ATO was issued and the ATO expires August 30, 2027.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Not Applicable.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

WingSwept is a SaaS solution hosted in the AWS GovCloud (US) and is approved to hold data at the FedRAMP and StateRAMP moderate level.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

<u>WingSwept Investigative module</u>

- Names of individuals involved in an investigation
- address
- SSN
- date of birth

• Financial information
• Job Title and Position

WingSwept Hotline module
• Name of individuals involved with or submitting a Hotline complaint, if not anonymous
• Personal/Work Phone Number & Email Address of individuals submitting a complaint, if not anonymous
• Addresses of individuals involved with or submitting a complaint, if not anonymous
• Job Title and Position

WingSwept AID module
• Names of individuals involved in an investigation
• Addresses of individuals involved in an investigation
• SSNs
• dates of birth
• Job Title and Position

2.2 What are the sources of the information and how is the information collected for the system?

For Hotline, Audits, and Investigations: Complainants who are employees of EPA; employees of other Federal agencies; employees of state and local agencies; and private citizens. Records in the system come from complainants through the telephone, mail, personal interviews, and Internet Web Site. Information is entered by the auditors, program evaluators, and investigators during the course of their audit or investigation.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Yes.

The auditors, program evaluators and investigators may store information from commercial sources or publicly available data during the course of their audit or investigation. The information is used as supporting documents, as part of their audit, program evaluation or investigation.

2.4 Discuss how accuracy of the data is ensured.

OIG ensures that information is relevant, accurate, timely and complete.
For the Audits/Assignments, Hotline, Investigation's modules, information may not be collected directly from the individual due to nature of the job. However, as investigators/auditors gather more information, they correct inaccurate or outdated information in WingSwept.

OIG has a Data Quality policy and procedure (004) that applies to all OIG employees. WingSwept users such as Managers and Special Agents in Charge certify/validate the data entered by the staff. In addition, security controls are implemented and reviewed annually to ensure data is protected from unauthorized access.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

There is a risk that unauthorized individuals may access the information within the system or use it for an unauthorized purpose.

Mitigation:

There is a risk that unauthorized individuals may access the information within the system or use it for an unauthorized purpose. The risk is mitigated by ensuring effective access controls are implemented, and only authorized personnel are granted access to the system. All data in the system is encrypted.

Section 3.0 Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

Yes.

Different levels of access, roles and permissions are implemented within the system. Only those users assigned to the audit, compliant, or investigation have access to the data.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

Access controls are documented in the CIO policy and procedures, CIO 2150-P-01.2. The specific procedures are documented in the WingSwept System Security Plan (SSP) for the AC-6 controls. Requests to access the system must be submitted via a ticket system by the user's supervisor or higher-level manager in the directorate chain to annotate approval to access the system. Additionally, requests to increase the user's privileges must be submitted via a ticket system by the user's supervisor or higher-level manager.

3.3 Are there other components with assigned roles and responsibilities within the system?

Yes, each module in the WingSwept application has its own access control levels to further restrict and manage the security of the system.

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

Only OIG employees will have access to the information system data; no external parties or non-OIG personnel have access to the system data. WingSwept system administrators will have access to the SaaS application that WingSwept is hosted on and maintain the information system. As an added layer of security, each CMTS customer operates in a secure environment with data separated and maintained by customer.

Yes, it included contractors who work for OIG. SAIC has their own onboarding process and includes non-disclosure agreements as well as agency FAR clauses.

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

Information is retained based on legal and federal requirements as described under the Inspector General Act of 1978, as amended, U.S.C. app. WingSwept uses the EPA Record Retention Schedule Controls and Oversight 1016 (audits, evaluations, and investigations).

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

There are risks of storing data past the retention schedule or reviews not performed to identify data to be retained or destroyed.

Mitigation:

OIG conducts an annual review of the information against the applicable RECORD SCHEDULE 1016.

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

The information is shared outside of EPA according to the routine uses outlined in the following SORNs:

EPA-30 OIG Hotline Allegation System
EPA-40 Inspector General's Operation and Reporting (IGOR) System Investigative Files

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

External sharing of OIG investigated files is designed to align with the original purposes of the collection by ensuring that the sharing of information supports the investigation and accountability processes. Disclosures are compatible with routine uses within the System of Records Notice (SORN) by adhering to established guidelines that define how and why information can be shared. The Memorandum of Understanding (MOU) outlines these guidelines, ensuring that any external sharing is conducted in a manner that respects privacy and legal requirements while facilitating necessary oversight and transparency.

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

The MOUs are reviewed and updated when there is a significant change or every 2 years.

4.4 Does the agreement place limitations on re-dissemination?

Information shared between the OIG and other organizations do not allow re-dissemination of data provided by the OIG.

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

Information shared across other local, state, and federal agencies can pose a risk if the information is mishandled or inadvertently leaked.

Mitigation:

All data within WingSwept is encrypted in transit and at rest. Additionally, due to the nature of the data any information shared externally is shared using encrypted USB's or secure file

transfer protocol (SFTP) and utilizes the latest encryption standard. PII incident handling is addressed in the MOUs and each organization has the responsibility to respond accordingly.

Section 5.0 Auditing and Accountability

The following questions are intended to describe technical and policy- based safeguards and security measures.

5.1 How does the system ensure that the information is used as stated in Section 6.1?

As documented in the WingSwept System Security Plan (SSP for the Monitoring and Auditing (AR) controls, the OIG Program Office utilizes the Risk Management Framework strategy and process to comply with privacy protection requirements and minimize the privacy risk to individuals. WingSwept is subject to annual third-party security assessments conducted by FAA. WingSwept team members perform regular reviews of login auditing to monitor access. It is also the Office of Inspector General's (OIG) responsibility for monitoring and auditing privacy controls and internal privacy policies on a continuous basis to ensure effective implementation of this procedure.

Additionally, the agency Privacy Office conducts annual reviews to evaluate the PII data collected and inquires whether PII data is still required. OIG responds to these annual FIS data calls that are used to determine if the collection of PII is relevant and necessary to accomplish the mission. These data calls assist in ensuring data collected and retained is for the specific documented purpose. In response to the FIS data call, the OIG re-evaluates the information collected and validates the need for that information.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

All EPA OIG staff take mandatory annual Information Security and Privacy Awareness Training. Additionally, when working in WingSwept, if a specific document contains PII, teams have been directed to label the electronic file as containing PII.

Additionally, investigators undergo additional training in accordance with OIG policy and procedures 202 and auditors take additional training in accordance with the yellow book standard. Staff have been instructed to include a statement at the beginning of the working paper in large letter “Contains PII”. (Exact wording varies by team).

The policy and procedure that staff follow regarding labelling of PII is OIG Procedure 413.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

There is minimal risk related to auditing and accountability in terms of changes to the configuration of the system. There is a likelihood that annual audits of systems (FIS) produce inaccurate results that exposes WingSwept and PII processed to threats. There is also minimal privacy risk that logging records contain PII, and that access logging could fail in relation to electronic records.

Mitigation:

The agency Privacy Office conducts a review (Privacy Impact Analysis) to evaluate the PII data collected and reviews whether certain data are still required.

OIG responds to the annual FIS data call that we are only collecting PII relevant and necessary to accomplish the mission. Data call responses are validated by SO and LPOs based on a baseline.

Data is only collected and retained for the specific use purposes.

Only authorized WingSwept administrators can effect changes to the configuration of the system.

Section 6.0 Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information.

In pursuant of the Inspector General Act of 1978, the OIG conducts independent audits, evaluations, investigations, and advisory services that promote economy, efficiency, and effectiveness; to prevent and detect fraud, waste and abuse in EPA programs.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes_X__ No___. If yes, what identifier(s) will be used.

For the WingSwept Investigations and WingSwept Hotline module, information is retrieved by personal identifier (i.e. case number, name, etc.).

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

PTA and PIA are conducted to address any privacy concerns related to the data contained within WingSwept. Safeguards are in place such as encryption of all data at rest and in transit in an event of accidental or intentional information disclosure. Further safeguards are in place such as access control lists to ensure only approved individuals have access to the

data. Additionally, WingSwept undergoes annual continuous monitoring assessment (CMA) to test security and privacy controls by an external assessor.

6.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk:

There are risks associated with unauthorized access or disclosure of information.

Mitigation:

OIG employees read, understand, and accept the rules of behavior. If they decline, will not have access to WingSwept. In addition, each time the user uses WingSwept, they are presented the OIG Systems Warning Notice which communicates system monitoring each time a user accesses the system (see below). The user is then prompted to either Agree or Decline.

WingSwept Systems Warning Notice:

Government Warning Notice

In proceeding to access this U.S. Government information system, you acknowledge that you fully understand and consent to all of the following terms and conditions:

1. You are accessing U.S. Government information and information systems that are provided for official U.S. Government purposes only.
2. Unauthorized access to or unauthorized use of U.S. Government information or information systems is subject to criminal, civil, administrative, or other lawful action.
3. The term U.S. Government information system includes systems operated on behalf of the U.S. Government.
4. You have no reasonable expectation of privacy regarding any communications or information used, transmitted, or stored on U.S. Government information systems.
5. At any time, the U.S. Government may for any lawful government purpose, without notice, monitor, intercept, search, and seize any authorized or unauthorized communication to or from U.S. Government information systems or information used or stored on U.S. Government information systems.
6. At any time, the U.S. Government may for any lawful government purpose, search and seize any authorized or unauthorized device, to include non-U.S. Government owned devices, that stores U.S. Government information.
7. Any communications or information used, transmitted, or stored on U.S. Government information systems may be used or disclosed for any lawful government purpose, including but not limited to, administrative purposes,

penetration testing, communication security monitoring, personnel misconduct measures, law enforcement, and counterintelligence inquiries.

8. You may not process, or store classified national security information on this computer system.
9. By using your PIV card to electronically sign Agency documents, you acknowledge that you have the same intent as would be required for an authorized handwritten signature to any Agency documents.

OIG users also take annual security training and for those with privileged access, at least two role-based security training per year. Regular users sign off on the rules of behavior while those with Privileged access, complete the Privileged User RoB.

***If no SORN is required, STOP HERE.**

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

This Privacy Impact Assessment serve as public notice in addition to the EPA-30 and EPA-40 System of Records Notices.

A Privacy Act Statement is provided at the point of collection..

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

During investigations individuals can refuse to provide information but are made aware of the legal consequences.

For the Hotline: information can be submitted anonymously.

7.3 Privacy Impact Analysis: Related to Notice

Privacy Risk:

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 claims Privacy Act exemptions for records maintained under INTERIOR/OIG-02, Investigative Records, pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), (k)(3) and (k)(5) that may preclude individual notice in order to protect law enforcement investigations

Mitigation:

This PIA and the published SORN provides constructive notice.

Section 8.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

8.1 What are the procedures that allow individuals to access their information?

Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16.

8.3 Privacy Impact Analysis: Related to Redress

Privacy Risk:

Inaccuracy or lack of current information could impact the integrity of OIG's mission and operations, as well as introduce privacy risk in the agency's privacy response capability. Response could be delayed when needed.

Mitigation:

Procedures for correcting information are published in the OIG SORNs 30, 40.