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: Inspector General Enterprise Management System	
Preparer: Alexander Stone	**Office: OIG, Office of Management**
Date: 08/05/2021	**Phone: 202-566-2472**

Reason for Submittal: New PIA____   Revised PIA____   Annual Review__X__ 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:

The Inspector General Enterprise System (IGEMS) is an application used by the auditors, program evaluators, investigators, and support staff to perform the EPA OIG mission. It contains major modules such as Assignments, Assignment Planning, Investigations, Hotline, Performance Management and Results, Project Management Actuals, Time planning, COOP Module, and OneBook. It is a restricted site accessible only by the government employees of the EPA OIG.

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. app. 3.

For the COOP Emergency Module, the authority to collect is from 42 U.S.C. 5121 et seq.; Executive Order 12656 (Nov. 18, 1989).

Refer to SORNs EPA-30 (Hotline), 40 (investigations), 42 (Audit/Timesheets) and 44 (COOP Emergency Contact Information).

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 issues and the ATO expires April 6, 2023

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.

No ICR required.

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?

No.

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).

As part of the investigative process, inside the Investigations and Hotline modules, the investigators store names, locations and other personal identifiers of individuals involved or participating in the OIG investigative process. Examples include names, social security numbers, date of birth, telephone number, and address of the people who submitted the Hotline information, the people who were reported and the OIG employees working on the hotline complaint and investigative cases. See SORN 30 and 40. Note SORNs 30 and 40 were updated and under review.

-       The COOP module contains EPA OIG employee emergency contact information. Examples include employee emergency address, telephone numbers and names of their emergency contact. See EPA SORN 44.

-       The Assignment module contains projects both audit, non-audit and general assignments used by the auditors to perform their audits and program evaluations. Examples are auditees, findings, monetary benefits, OIG employees who perform the audits, time charged to the projects, individuals who requested audits or special projects, names of individual auditees.

-       The Project Management Actuals (formerly Timesheets) contain OIG employees hours charges to direct and indirect projects.

-       The Time planning module contains submitted/approved planned timesheets (requests for hours, telework, employee wellness program leave).

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. Because security cannot be guaranteed on the Internet site, complainants are advised that information they provide through the Internet site may not be confidential. Information is entered by the auditors, program evaluators and investigators during the course of their audit or investigation.

For the COOP module, the OIG employees enter their own emergency contact information.

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

Not directly. 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 IGEMS.

For the COOP module, IGEMS collects the PII directly from OIG employees. They update/correct information as needed.

OIG has a Data Quality policy and procedure (004) that applies to all OIG employees. IGEMS 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 are risks associated with unauthorized access or disclosure of information or inaccurate data.

Mitigation:

As a whole, IGEMS system is accessible to EPA OIG employees only. It is an internal application accessible by multi-factor authentication. Use of strong passwords, which are renewed on a regular basis, and screen locks are enforced. In addition, there are different levels of access, roles and permissions implemented inside IGEMS. Only those users assigned to the audit, complaint or investigation have access to the data.

Security controls are implemented and reviewed annually. Continuously monitoring assessment are conducted.

From SORN 40 – updated:

The IGEMS Investigations module (I2M) is restricted to the I2M Administrator and the staff of EPA OIG Office of Investigations, Office of Counsel, the Inspector General and Deputy Inspector General. It is one of the modules found in IGEMS.

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?

In pursuant of the Inspector General Act of 1978, the Office of Inspector General conducts independent audits, program evaluations, investigations and advisory services that promote economy, efficiency, and effectiveness, and help to prevent and detect fraud, waste, and abuse in EPA programs.   IGEMS is the system/tool that the auditors, program evaluators and investigators use to store the data they collected. Access to individual modules is granted by supervisor approval and managed using Active Directory group membership.

For the Hotline Module (SORN-30):

Fulfills OIG's responsibilities under Section 7 of the Inspector General Act, that is to receive and investigate complaints of information concerning the possible existence of activities constituting a violation of law, rules or regulations, mismanagement, gross waste of funds, abuse of authority or a

substantial and specific danger to the public health or safety, and the subject of the complaints.

For the Investigations Module (SORN-40): To serve as the repository of information collected in the course of conducting investigations relating to programs and operations of the EPA.

For the Audit, Assignment and Project Management Actuals (formerly Timesheets SORN-42): To assist the OIG in planning and managing audits, evaluations, investigations, and other OIG activities.

For the COOP (Emergency Contact) Module (SORN EPA-44): To contact employees, in case of an emergency or other event that may require their assistance.

Access to individual modules is granted per job requirements. i.e .auditor or investigator. Access is granted using Active Directory group membership

Refer to revised SORNs EPA-30, 40, 42 and 44.

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 IGEMS 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 IGEMS Module in the IGEMS 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; no external parties or non-OIG personnel have access to the system.

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. IGEMS uses the EPA Record Retention Schedule 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:

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.

No information is shared outside of the EPA OIG.

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

Not Applicable (N/A)

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?
Not Applicable (N/A)

4.4   Does the agreement place limitations on re-dissemination?
Not Applicable (N/A)

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:
None. Information is not shared externally.

Mitigation:

None

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 IGEMS 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. IGEMS is subject to annual third-party security assessments conducted by FAA. IGEMS 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 IGEMS, if a specific document contains PII, teams have been directed to label the electronic file as containing PII. 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 labeling 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 changes to the

configuration of the system.

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 is only collected and retained for the specific purpose.

Only authorized OIG 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. *(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.)*

For the COOP module, information retrieved about the user are the emergency contact information.

For the Investigations and Hotline, information retrieved about them are their assigned cases or complaints. If the user is the subject of the investigation, they will not have access to the investigative data.

For the Assignment Module, information retrieved about the user are their assignment projects and their time charges for the projects.

For the Training Module, information about IDPs and training requests.

For the Time planning Module, planned hours for the pay period.

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?

IGEMS is subject to annual third-party security assessments conducted by FAA. IGEMS 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.

6.4   <u>Privacy Impact Analysis</u>: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

<u>Privacy Risk</u>:

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

<u>Mitigation</u>:

OIG employees read, understand, and accept the rules of behavior. If they decline, will not have access to IGEMS. In addition, each time the user uses IGEMS, 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.

OIG Systems Warning Notice:

In proceeding and accessing U.S. Government information and information systems, you acknowledge that you fully understand and consent to all of the following:

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; and

8.   you may not process or store classified national security information on this computer system.

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.

EPA OIG employees are presented with the OIG Systems Warning each time prior to accessing IGEMS. They have to option to accept or decline. If they decline, they will not be able to access IGEMS.

IGEMS also has SORNs (EPA-30, 40, 42 and 44). National Privacy Program (NPP) publishes all final privacy documents on agency's Privacy internet and intranet sites.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

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?

EPA OIG employees are presented with the OIG Systems Warning prior to accessing IGEMS. They have to option to accept or decline. If they decline, they will not be able to access IGEMS.

Refer to SORNS: EPA 30, 40, 42, 44. IGEMS data is not accessible by the public.

See also EPA's Information Security-Privacy Procedure.

Users have the option of declining the system rules of behavior. In the COOP Module, users have the option to enter their personal phone and home address. They also have the option of indicating

their personal phone unlisted.

Individuals are allowed to consent to collection, use, and maintenance of information in the system.

Individuals are provided an opportunity to consent to the information collected or uses/ third-party sharing.

Users entering the information identify incorrect information in performance of duties and can correct information.

7.3   <u>Privacy Impact Analysis</u>: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

<u>Privacy Risk</u>:

There are potential risks of users and individuals not reading the OIG System Warning Notice or accessing the SORNs.

<u>Mitigation</u>:

The OIG Systems Warning Notice is presented to the IGEMS users each time they access IGEMS. OIG employees complete training on security/privacy yearly. Others with privileged access have to take additional role-based security training.

OIG employees are reminded yearly to update their COOP emergency information.

IGEMS is restricted to EPA OIG government employees. SORNS are published

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?

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted. 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

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

None.

Mitigation:

For the COOP module, managers send a reminder to their staff yearly to confirm their COOP emergency information.

Procedures for correcting information are published in the OIG SORNs 30, 40, 42 and EPA – 44)