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 (IGEMS)	
Preparer: Calvert Acklin	**Office: OIG, Office of Management**
Date: April 24, 2020	**Phone: 202-566-9856**
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.

Yes. The ATO expires on April 6, 2020 (currently extended until the May ATI review).

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 may 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).

The Training module contains OIG employees IDPs, and requests for training.

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, Investigations 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?

Yes, IGEMS has access control levels implemented. It will only allow access to individuals based on the requirements of their job.

IT support staff that require privileged access use the agency's elevated rights request system. All elevated privileged requests require justification with approval by the person's supervisor or manager, OIG ISO, and OIG IMO.

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

They are identified in the IGEMS SSP.

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

Yes. Each module has its own access control levels further tightening 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 internal government personnel have access to the IGEMS modules.

Information Sharing of PII data is only shared as identified in IGEMS SORNS 30,40,42 and 44.

If appropriate, OIG will have the proper MOU and ISA, reviewed by the NPP, to allow the sharing of IGEMS data with external parties.

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.

IGEMS uses the EPA Record Retention Schedule 1016 (audits, program evaluations and investigations). Disposition description: **"**b) IG investigative case files for cases that document investigations of known or alleged fraud, abuse, irregularities, and violations of laws and regulations involving EPA personnel, programs, or operations administered or financed by EPA, including contractors and others having a relationship with EPA, and excluding cases covered by item a. and 1006 for Project Management Actuals.**"**. NARA Disposal Authority: DAA-0412-2013-0015-0002. Disposable: Close when audit is complete or case is closed; destroy 20 years after file closure.
Disposition c: Routine controls and oversight records includes, but is not limited to:

- Administrative documentation related to the audit resolution process;
- Audit case file final reports and work papers maintained by the headquarters IG or other auditing organization;
- IG hotline files, including complaints, correspondence with responsible officials, synopses of cases, and monthly and periodic workload and trend reports;
- IG or other auditing organization management assessment reviews and program evaluations of the auditing organization's procedures or programs for economy, efficiency, and compliance with policies and professional standards;
- Laboratory performance evaluation studies proficiency testing (PT) records relating to how well laboratories perform, including studies, performance evaluation reports,

performance summaries, statistical reports, method-specific studies, and related records;

- Responses to audits, evaluations, and investigations maintained by the office being investigated, evaluated or audited, conducted internally (e.g., by IG), or externally (e.g., by Government Accountability Office) and that may be initiated by EPA, an outside agency with oversight over EPA, or requested by Congress, and records related to the Federal Managers Financial Integrity Act (FMFIA); and
- State and other entity relations and oversight files, including records used to oversee programs operated in lieu of a federal program.
- NARA Disposal Authority: DAA-0412-2013-0015-0003. Disposable: Close when case is closed, or activity or report is completed or superseded. Destroy10 years after file closure.

Records Schedule 1006 for Project Management Actuals:
Disposition description b: Other administrative management records includes, but is not limited to:

- Calendars, schedules, and logs of daily activities containing substantive information regarding daily activities for federal employees other than senior officials;
- Committee and internal staff meeting records, including agendas, meeting arrangements and minutes, final reports and related records created by or documenting the accomplishments of intra-agency and internal committees and workgroups;
- Copies and background materials related to Circular No. A-76 maintained by offices other than the office having primary responsibility:
- EPA forms and supporting materials showing inception, scope and purpose;
- Final deliverables and reports related to administrative activities;
- General correspondence files, including non-controlled correspondence relating to work assignments, personnel needs, and other routine activities of the office;
- Program management files maintained by other than senior officials related to the on-going management of mission and operational programs and projects, including correspondence, staff meeting records, routine office procedures, reports related to general policy and program matters (e.g., Superfund Comprehensive Accomplishment Plan (SCAP) reports), oversight reviews, interagency activities, routine management of environmental management systems (EMS), and project files showing assignments, progress, and completion of projects;
- Records management documentation, including records inventories, records disposal, requests for disposition authority, transfer authorizations;
- Routine office management records, including activity, progress, statistical, and workload reports, office staffing, procedures, communications, services (e.g., printing, post office, private mail, delivery, transportation and freight companies), supplies and equipment, expenditure and disbursement of funds (e.g., employee transportation subsidies), budget papers; and
- Time and attendance source and leave records maintained by timekeepers, including time and attendance records such as time or sign-in sheets, flexitime records (e.g., biweekly maxiflex schedules), leave applications for jury and military duty, authorizations for premium pay or overtime, supervisor time sheet certifications, and related documents.

NARA Disposal Authority: DAA-0412-2013-0011-0002. Disposable: Close when discontinued, superseded, or canceled, or when no longer needed for current agency business. Destroy 6 years after file closure.

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:

IGEMS has reached a maturity point where some data are due for destruction. Module managers are contacted to confirm records that need to be destroyed or transferred to NARA.

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.

Any information shared outside of the IGEMS system is documented in IGEMS SORNS 30,40,42 and 44.

If appropriate, OIG will have the proper MOU and ISA, reviewed by the NPP, approved for any external sharing.

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

Any external sharing is compatible with the purposes documented in the SORNs (30, 40, 42 and 44).

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?

All ISAs and MOUs require review and approval by OIG Legal Counsel, the shared entity, and OIG management, and must be compatible with the original purpose of the system as documented in SORNs 30, 40, 42, and 44).

4.4 Does the agreement place limitations on re-dissemination?

Limitations are specified in the related SORNS for EPA-30, 40, 42, and 44. Further limitations are by the EPA on the public privacy site at: https://www.epa.gov/privacy/how-epa-implements-privacy-act

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:

There are risks associated with sharing of information outside of the agency by internal personnel not following OIG, agency, and federal privacy laws.

Mitigation:

OIG personnel and authorized IGEMS users are required to take information security and privacy awareness training course when coming onboard and annually thereafter. Personnel are also required to sign and acknowledge rules of behavior when onboarding and annually through the IGEMS module. Auditors and investigators require additional certifications in conducting audits and investigations, which is documented in

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?

There are audit log in use…

OIG security performs monthly compliance monitoring of daily activity. Monitor event logs as required by EPA security policy. These weekly reviews are certified on a monthly report to the OIG security officer, IMO and SIO.

•Check log for consecutive invalid login attempts (Maximum is 3)

•Check date and times of log on and log off events

•Check for system configuration changes, specifically any that occurred outside of the change control process

•Check for the activation of intrusion detection and anti-virus/malware programs

•Check for exceptions including connection errors, system restarts, system availability, system tolerance.

•Check application and database related status codes and related requests unusual activity such as an unexpected increased number of requests and unexpected status changesOnly authorized OIG administrators can effect changes to the configuration of the system.

In addition to the above auditing, IGEMS administrators review the roles assigned to the users and managers on a monthly basis to determine if updates to personnel access are required by working with the auditing and investigation managers. Managers in turn monitor auditor assignments and modify access accordingly.

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

IGEMS users are mandated to complete the yearly information security and privacy awareness training. In addition, for those with privileged access, they are mandated to complete the role-based training. Those with Top secret clearances complete the NSI Security training. Completion of the training are part of their performance standard.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Despite mandated training, insider threat is always a risk, as well as unintended disclosure of data.

Mitigation:

The OIG and agency monitor user activity, and OIG IT personnel undergo annually incident response training in addition to information security training.

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 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.

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.

Refer to additional information in the published or revised SORNs EPA-30, 40, 42 and 44.

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.)

The methods of retrieval are defined in each SORN.

SORN 40 - Investigations Module: By names and other identifiers of subjects, complainants and witnesses interviewed during investigations; others involved in the investigative process; and investigative case file numbers.

SORN 30 - Hotline Module By case number, complainant or subject name, and subject matter.

SORN 42 - Audits, Assignments, Timesheets (Project Management Actuals): By assignment number, audit report number, the name of the assigned OIG auditor, or the name of the audit requestor. The general assignment module contains records that are retrieved by assignment number and the name of the OIG employee performing the assignment.

For the COOP Module - By employee name.

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?

The information associated with individuals and contained in the IGEMS originates from interviews, notes, and documentation provided as part of an audit, evaluation, review, or investigation. Access is restricted to OIG auditors, evaluators, special agents and their managers, and information is not accessible to the public nor shared externally. Access to IGEMS files is controlled by the audit and investigative managers and only provided to as assigned to a particular audit, evaluation, or investigation.

6.4 Privacy Impact Analysis: 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.

Privacy Risk:

There are risks associated to unauthorized access or use of information

Mitigation:

The audit logs mentioned in section 5.1 are reviewed on a monthly basis to ensure only authorized personnel are accessing the approved assignments

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.

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.

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

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 Privacy Impact Analysis: 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.

Privacy Risk:

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.

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

Mitigation:

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.

IGEMS data is not accessible by the public. Record access procedure is published via SORN. IGEMS is an exempted system.
SORN 30 (Hotline), 40 (Investigations), Record Access Procedure: To the extent permitted under the Privacy Act of 1974, 5 U.S.C. 552a(k)(2), this system has been exempted from the provisions of the Privacy Act of 1974 that permit access and correction. However, EPA may, in its discretion, fully grant individual requests for access and correction if it determines that the exercise of these rights will not interfere with an interest that the exemption is intended to protect. The exemption from access is limited in some instances by law to information that would reveal the identity of a confidential source. Requesters will be required to provide adequate identification, such as a driver's license, employee identification. card, or other identifying document

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.

We have a provided a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and

We established a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.

As stated in the Contesting Procedure in the OIG SORNS EPA-30, 40, 42, EPA-44 (same for Hotline, Investigations, Audits/Timesheets and COOP Emergency modules)

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 outside of the agency's Privacy Act and FOIA processes.

Mitigation:

Refer to OIG SORNs 30, 40 and 42, and EPA-44. There are clearly defined procedures in the SORNS that discuss records access and contesting records.