PRIVACY IMPACT ASSESSMENT

Submit in *Word format* electronically to: Linda Person (person.linda@epa.gov)

Office of Environmental Information

System Name: The Inspector General Enterprise Management System (IGEMS) - Full	
Preparer: Maria Martir	**Office: OIG**
Date: 10/2016	**Phone: 202-566-2692**
This project is in the following life cycle stage(s):	
Definition □ Development/Acquisition □	Implementation □
Operation & Maintenance ☒ Termination □	

Note: Existing Systems require an updated PIA when there is a significant modification or where changes have been made to the system that may create a new privacy risk. For a listing of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f) at http://www.whitehouse.gov/omb/circulars/a130/a130appendix_i.aspx

I. Data in the System

1. What data/information will be collected/contained in the system?

The integrated system, Inspector General Enterprise System (IGEMS) feature the following modules; project management, case and hotline management, project analysis, resource management (which includes users name, and work hours), knowledge management/collaboration management, project/cost accounting, workflow management, document management, reports and analysis, time management, and COOP (emergency) data management.

IGEMS use single-sign on by using the EPA's Personal Identification Card (PIV) as a means of authentication. It is associated with the authenication method used for granting use of the EPA network. IGEMS only allow OIG personnel to access the system. The access control is also controlled by applicatoin roles and permissions. To gain access to the computer after its locked after three failed attemps, the user must contact OIG Technical Support Team for them to unlock / reset Active Directory (AD) accounts.

- The Investigations and Hotline modules contain names, locations and other personal identifiers of individuals involved or participating in the OIG investigative process. Examples include names, social sercurity numbers, date of birth, telephone number, and address.

- The COOP module contains EPA OIG employee emergency contact information.

- The Assignment module contains the Office of Inspector General (OIG) employees; individuals who request audits or special projects; names of individual auditees.

2. What are the sources and types of the data/information in the system?

The data sources of the privacy information are EPA OIG investigators, auditors, program evaluators, Hotline manager, OIG managers and staff. IGEMS contains information relating to audits, evaluations, investigations, hotline complaints and COOP emergecy contact information for EPA OIG employees.

3. If the system has been modified, are the original personally identifiable information (PII) elements still being collected or contained in the system? If no, what are the elements currently being collected? When did the collection of the original PII elements stop? How was the old data removed from the system?

IGEMS undergoes upgrades and enhancements. Original PII information from audits, investigations and hotline complaints are maintained in the system. Exiting EPA OIG employee's emergency information is removed from the system.

4. How will the information be used by the Agency?

IGEMS automates the workflow, tracks projects, cases, and cost information associated with problems, abuses, and deficiencies relating to EPA programs and operations, as well as progress of corrective actions that are reported to the EPA Administrator and Congress. IGEMS also monitors project progress and tracks measures and results. Data is used to support EPA OIG mission and goals in pursuant of the Inspector General Act of 1978.

5. Why is the information being collected? (Purpose)

The EPA Office of Inspector General (OIG) uses IGEMS data to report on the efficiency of EPA programs and operations.

The OIG provides independent audit, evaluation, investigative and advisory services that promote economy, efficiency, and effectiveness, and help to prevent and detect fraud, waste, and abuse in order to add value in EPA programs and operations. The OIG has further interpreted this statutory mission through its strategic and annual performance goals for contributing to environmental quality, human health, and good government in order to inspire public confidence in the integrity of EPA operations. The COOP (emergency) contact information of OIG personnel are collected to contact employees in case of an emergency or other event that may require their assistance.

II. Access Controls for the Data

1. To ensure user authentication, does the system have limited login attempts or require security question answers? If yes, when the user becomes locked out how will they gain access to the system?

Yes, the system is limited to 3 login attempts before account lock out via the agencies active directory group policy. To gain access to the system after locked, either the OIG's Technical Support team or the agency's help desk must be contacted.

2. How often are passwords required to be changed?

Passwords are required to be changed every 90 days based on the agency's policy.

3. Who will have access to the data/information in the system *(internal and external parties)*? If contractors, are the Federal Acquisition Regulations (FAR) clauses included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act)?

EPA OIG employees have access to the data based on their position on the organizational structure and roles granted to them. There are a few individuals such as the database administrator and IGEMS Administrators who have more access to the data.

4. How will you educate individuals/users having authorized access about the misuse of PII data? Will users receive privacy training before gaining access to the system?

Users sign the Rules of Behaviour (ROB) agreement and take annual training on IT Security Awareness and PII. Users also follow a procedure for requesting access/ release of data.

5. Has the data in the system been encrypted according to the National Institute of Standards and Technology (NIST) requirements? (Note: this requirement is for sensitive PII only)

Yes, the data is being encrypted during the backup process according to NIST standards. The data is not encrypted at the database level (data at rest) but we use the Secure Socket Layer web server certificates to encrypt the PII data in transit.

6. Do other systems share or have access to information in this system? If yes, who authorized the sharing? If information is being shared, please provide a copy of any agreements that were issued. *(i.e., System Administrators, System Developers, System Managers)*

Yes, the Management Audit Tracking System (MATS) interfaces with IGEMS. A representative from the Office of Planning, Analysis and Accountability, Office of the Chief Financial Officer, EPA, has access to audit data which feeds into MATS (One way push). Access is strictly to MATS-related data. There is an existing Memorandum of Understanding (MOU) and Interconnection Security Agreement (ISA) signed 10/22/2014 between representatives of OIG and OCFO. This person has her own account to the DB.

7. Will other agencies, state or local governments, or other external parties (i.e., non-EPA) share or have access to information in this system? If so, what type of agreement was issued? (*i.e., ISA, MOU, etc.*) *(If any agreements were issued, the Privacy Program needs a copy for its records)*.

No.

8. Will data and/or processes be converted from paper to electronic? If so, what controls are in place to protect the data from unauthorized access or use?

No.

9. Will data be shared from a system of records (SOR) with another federal agency? If so, has a computer matching agreement been initiated?

No.

III. Attributes of the Data

1. Explain how the use of the data is both relevant and necessary to the purpose for which the system is being designed. (*Provide an example or explain)*

The data collected is relevant and necessary to track individual audit, program evaluation, and investigative assignments, time, and cost associated with the OIG assignments. IGEMS is an application that supports EPA OIG mission and goals.

2. How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? 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.*)

Access to IGEMS is restricted to EPA OIG employees. IGEMS uses Active Directory credentials to authenticate the user. It uses the user's position in the organization and special roles and privileges to authenticate the user and restrict access. In addition, IGEMS uses SSL Web Server certificates to secure the server and encrypt transmission of data.

In the Assignments and Timesheets module, data may be retrieved by employee names or assignment numbers.

In the COOP module, data may be retrieved by organizational chain.

3. Has the system undergone a risk analysis to identify harms that may result from technical failures, malevolent third parties or human error? Yes___ No___ (**Note: The risk analysis will help identify possible risks to the data in the system.**)

Yes.

4. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the requested information? Yes___ No___ If yes, how is notice given to the individual? *(Privacy policies must clearly explain where the collection or sharing of certain information may be optional and provide users a mechanism to assert any preference to withhold information or prohibit secondary use.)*

Yes. IGEMS has Rules of Behaviour (ROB) for all users. Each user has an opportunity to accept or decline the set of rules. If the user declines, the user does not get access to any IGEMS data.

5. Where is the on-line privacy policy posted?

A privacy policy warning note is displayed at the application logon screen.

IV. Maintenance and Administrative Controls

1. Has a record control schedule been issued for the records in the system or the system itself? If so, provide the schedule number. *(You may check with the record liaison officer (RLO) for your AA-ship or Tammy Boulware, Headquarters Records Officer, to determine if there is a retention schedule for the subject records. All systems **must** have a record control schedule.)*

Yes, IGEMS is covered under EPA Records Schedule 1016.

2. While the data are retained in the system, what are the requirements for determining that the information collected remains sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

The managers review the data for accuracy prior to making decisions. The OIG developed a data quality policy which ensures that proper management responsibilities are in place to comply with EPA's Information Quality Guidelines (OMB Section 515). Annually, the Deputy Inspector General of the OIG certify as a part of the OIG Annual Performance Report, that all data reported through OIG information systems meets the EPA data quality standards.

In addition, IGEMS generate management reports such as monthly status, assignment costs, and quality assurance reports, which serve as tools for reviewing data accuracy.

3. Will this system provide the capability to identify, locate, or monitor individuals? If yes, explain.

Yes, IGEMS provides the capability to identify, locate, or monitor individuals by tracking each user to OIG audits and investigative cases and hotline complaints.

4. Does the system use any persistent tracking technologies?

No.

5. Under which System of Records (SOR) notice does the system operate? Provide the name of the system and its SOR number if applicable. All Agency SORs are posted at http://www.epa.gov/privacy/notice/. *(A SOR is any collection of records under the control of the Agency in which the data is retrieved by a personal identifier. The SOR **must** contain the same categories of records and cover the same routine uses as your system.)*

a. Inspector General Enterprise Management System (IGEMS) Investigative Module, EPA-40

b. Inspector General Enterprise Management System (IGEMS) Hotline Module, EPA-30

c. Inspector General Enterprise Management System (IGEMS) Audit, Assignment and Timesheet Modules EPA-42

d. EPA Personnel Emergency Contact Files EPA-44 – Covers OIG (IGEMS) COOP Module