

# 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](https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx)

<b>System Name: OIG_DAE -Data Analytics Enterprise</b>	<b>System Owner: Adam Seefeldt</b>
<b>Preparer: Alexander Stone</b>	<b>Office: OIG-OSAR</b>
<b>Date: 01/04/2024</b>	<b>Phone: 202-566-2472</b>
<b>Reason for Submittal: New PIA</b> <input type="checkbox"/> <b>Revised PIA</b> <input checked="" type="checkbox"/> <b>Annual Review</b> <input checked="" type="checkbox"/> <b>Rescindment</b> <input type="checkbox"/>	
<b>This system is in the following life cycle stage(s):</b>	
Definition <input type="checkbox"/> Development/Acquisition <input type="checkbox"/> Implementation <input type="checkbox"/>	
Operation & Maintenance <input checked="" type="checkbox"/> Rescindment/Decommissioned <input type="checkbox"/>	
<b>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 <u>OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).</u></b>	
<b>The PIA must describe the risk associated with that action. For assistance in applying privacy risk see <u><a href="#">OMB Circular No. A-123, Section VII (A) (pgs. 44-45).</a></u></b>	

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

The system and database will be used by data analysts to perform trend analysis, outcomes, etc to supplement required reporting to OIG. The system will gather information from various systems (Grant, Contract, Auditing). The database will utilize Structured Query Language (SQL) to obtain information from various systems.

## **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?**

EPA Office of Inspector General (OIG) mission and goals pursuant to the Inspector General Act of 1978, 5 U.S.C. app.

### **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?**

The database and production servers for DAE are hosted within TSEC (GSS) environment. The ATO for DAE is currently pending approval post FY24 CMA assessment.

### **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).**

Data analysts will use the Microsoft SQL database to ingest data which the data analysts will use to construct products which may show trends, outcomes, etc. that will be utilized to augment OIG reporting. Data elements ingested into the database will come from systems that contain grant, contract, and accounting information. Data collected could potentially include but is not limited to PII in the form of names, telephone numbers, email addresses, etc. and may include sensitive PII such as DOBs, financial records, and SSNs.

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

The database will collect data from existing Agency and OIG systems containing internal grant, contract, and accounting systems.

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

No

**2.4 Discuss how accuracy of the data is ensured.**

The database utilizes input validation to verify data is ingested accurately. The accuracy of the data is confirmed on the primary source system.

**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:**

Moderate risk attaches to the sensitive information in DAE, not only because some of it is SPII, but also because it pertains to investigations about fraud, waste or abuse and implicates individuals' reputations. Leakage of unproven claims about criminality or unethical behavior can harm an individual's reputation\_which is a privacy risk that we must address. The privacy risks associated with the sources of data include but not limited creditability/accuracy of public data and data obtained during investigations and or malicious claims made on the hotline in relation to fraud, waste and abuse by individuals.

**Mitigation:**

The DAE database is an internal database used by EPA OIG employees only. Only staff with a need to use the system are provided access.

The data contained within DAE is encrypted at rest and in transit.

Authentication to the system occurs through the agency's Active Directory Domain Controller. A user must have a strong password (combination of alpha-numeric-symbolic of at least 12 characters

in length) that are changed a minimum of every 60 days. Also, all devices that connect to the system use a screen lock; both (screen lock and password) are enforced by agency policy.

Additionally, all users must take annual mandatory Security Awareness and Privacy training and annual CUI training as provided by the agency.

## **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. Authentication and authorization to the database occurs through the agency's Active Directory Domain Controller, and access is restricted by group membership. Users are granted read and write access through the use of group membership and use their PIV or network credentials to log into the database.

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

CIO 2150-P-01.2-Information Security-Access Control Procedure. This policy establishes the EPA Information Security Program.

The procedures cover all EPA information and information systems, to include those used, managed or operated by a contractor, another agency or other organization on behalf of the EPA.

The procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of the EPA.

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

Yes. The IGEMS system has other components that restrict access based on assigned roles and responsibilities.

### **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 appropriate OIG Employees will have access to the database. No external parties or

non-OIG personnel have access to the database. No contractors will have access. Only OIG Employees (Feds).

**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.**

The information is retained for the minimal period specified in the EPA Record Retention Schedule 1016 (audits, evaluations, and investigations) for 10 years, and for the reason of conducting independent investigations as specified in the Inspector General Act of 1978, 5 U.S.C. app

**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 is maintained in accordance with EPA Record Retention Schedule 1016 (audits, evaluations, and investigations) for 10 years.

## **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 sharing outside of EPA is anticipated at this time.

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

External sharing is not anticipated at this time.

**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?**

Sharing of information is not anticipated at this time.

**4.4 Does the agreement place limitations on re-dissemination?**

No agreements are required at this time.

**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. No information is shared.

**Mitigation:**

Not applicable (N/A)

**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 DAE Security Plan, the Office of Inspector General's (OIG) conducts monitoring and auditing (part of AR controls) in accordance with EPA policy. 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. DAE is subject to annual third-party security assessments conducted by FAA. DAE team members perform regular reviews of login auditing to monitor access. It is also the IOG's responsibility for monitoring and auditing privacy controls and internal privacy policies using IG metrics across the enterprise on a continuous basis to ensure effective implementation of this procedure.

The agency National Privacy Office also 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. Staff determined to have significant security responsibilities are also required to complete annual role-based training (RBT).

## **5.3 Privacy Impact Analysis: Related to Auditing and Accountability**

### **Privacy Risk:**

Auditing records could be deleted or modified by authorized user and non-authorized users.

### **Mitigation:**

Auditing and accountability are performed by the system. All modifications and access to the database are logged and stored off the system in an alternate Security and Event Monitoring System (SIEM). Only authorized OIG employees will have access to the database.

## **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.**

The database will be used to perform trend analysis, outcomes, etc to supplement required reporting to OIG.

### **6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes\_\_ No\_X\_. 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.)**

Information within the database will be retrieved using SQL queries. There are no pre-defined dropdown options that would allow for data retrieval using personal identifiers. The databases will provide the underlying data for Power BI dashboards that will be hosted/published via Power BI Report Server to OIG personnel for audits, evaluations, investigations, and workforce metrics. The published dashboards might contain filters using PII/SPII data that

would allow the end user to search datasets using personal identifying information. Social security numbers, bank accounts, phone numbers, email addresses, medical, address information, and other personal identifiers could be used as searchable filters for published dashboard.

### **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?**

Evaluations are conducted on the source system and identified in the related SORNs for that system. The database will have technical controls in place that will ensure that only specified people with need to know will have access to the database.

### **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 with unauthorized use of information. Although DAE does not currently retrieve data using personal identifiers (currently retrieved using SQL queries) there is a potential risk associated with PII elements appearing in SQL queries in the future. Note-DAE does not collect PII but contains PII that is pulled from other systems.

#### **Mitigation:**

While data is not retrieved using personal identifiers because DAE is a computing environment, EPA-100 SORN provides the controls to mitigate potential risk associated with data retrieval using PII.

**\*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.**

DAE does not collect information but pulls it from other systems that have SORNs. DAE

also has SORN (EPA-100). 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](mailto: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?**

DAE is not a primary data collection point but only a repository of data collected from other systems.

### **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:**

Data processed within DAE is pulled from other systems and might not be covered by EPA-100. Privacy risk is associated with potentially insufficient notice to public.

#### **Mitigation:**

The potential insufficiency of notice for DAE, is addressed by published SORNs for the other systems in which it collects data from.

## **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:**

Procedures for correcting information are published in the OIG SORN EPA-100