

# 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:</b> DMAP	
<b>Preparer:</b> Shane Knipschild, Sileshi Desta, ISSO	<b>Office:</b> OMS-OIM-IAASD
<b>Date:</b> 04/11/2023	<b>Phone:</b> (202) 566-2712, (202) 564-0378
<b>Reason for Submittal:</b> New PIA____ Revised PIA___ Annual Review_X___ Rescindment ____	
<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>OMB Circular No. A-123, Section VII (A) (pgs. 44-45).</u></b>	

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

The purpose of this revised PIA is to initiate a process so that sensitive data may be added to the DMAP environment, which will be used for data retrieval purposes and therefore trigger the need for a SORN for DMAP. The data elements to be added include PII and other sensitive elements, and these will be managed as a group in a COTS Esri portal and referred to as GeoSecure.

EPA DMAP system is an AWS Cloud service software platform available to all agency employees as a collaborative shared service. This environment allows EPA users to transform data into actionable intelligence and automate workflows by connecting to various data sources. Like Microsoft's SharePoint offering, the DMAP system allows users to maintain control over the workspaces created for them and share their data with end users. The sources for data used by each content user are both internal and external databases and websites.

DMAP:

- Allows EPA to share data across the agency to inform national and regional issues
- Provides tools to load data from many sources
- Provides a focal point to integrate and analyze multiple data sources and file types
- Offers a centralized "hub" for EPA teams to discover and share data insights
- Accessing the EPA's DMAP platform requires EPA LAN Credentials

## **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?**

- 44 U.S.C. § 3506, Federal Agency Responsibilities;
- Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource;
- 5 U.S.C. 301, Departmental Regulations;
- 40 U.S.C. 1401, the Clinger-Cohen Act; and
- 44 U.S.C. 3541 et seq., Federal Information Security Modernization Act of 2014
- Public Law 107-347: A security plan must be developed and practiced throughout all life cycles of the agency's information systems.

### **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?**

A System Security Plan (SSP) has been completed for the DMAP system and is placed in XACTA. A Security Impact Analysis (SIA) has been completed as part of the documentation updates for a Moderate system. DMAP is currently classified as a Moderate system and has an approved ATO at that level. ATO expires 11/10/2024.

### **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. ICRs are the responsibility and covered under the individual Programs.

#### **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?**

Yes, DMAP is in Amazon cloud and is FedRAMP approved. The Cloud will include PaaS, IaaS and SaaS.

## **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).**

During the System Categorization process, system administrators identified at least 60 types of information that may be processed and stored in DMAP. These data types will be documented.

The following PII elements may exist within the datatypes processed or analyzed on the DMAP system:

- Names
- Phone numbers
- Business Addresses
- E-mail addresses
- CBI – Confidential Business Information

Here are some specific examples of data types and data elements we anticipate onboarding:

#### **EPA-Occupied Facilities (PII)**

- CONTACT\_EMAIL ( *type: esriFieldTypeString, alias: Contact Email, length: 100* )
- CONTACT\_EXTENSION ( *type: esriFieldTypeString, alias: Contact Extension, length: 10* )
- CONTACT\_NAME ( *type: esriFieldTypeString, alias: Contact Name, length: 100* )
- CONTACT\_PHONE ( *type: esriFieldTypeString, alias: Contact Phone Number, length: 50* )
- CONTACT\_URL ( *type: esriFieldTypeString, alias: Contact Website, length: 5000* )

#### **Drinking Water Surface Intakes, Source Water Areas, Public Water Systems, and Well Locations (Sensitive)**

- latitude and longitude coordinates of all Public Water Systems (PWS) source facilities (i.e., drinking water wells, surface water intakes, and other facilities categorized as “Sources” in SDWIS) and GIS analyses derived from these data from which a precise location can be determined.
- latitude and longitude for public water system treatment plant locations;
- delineated source water areas (SWA) polygons and related state source water assessment program (SWAP) data available to EPA.

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

The sources for data used by each created user come from both internal and external databases.

## **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, data sources may include both publicly available data and commercial sources. These data may be used in analytics and mashups designed for internal sharing in the case of sensitive data and sometimes public sharing in the case of non-sensitive data.

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

The accuracy of the data is not ensured through any automated means. This data depends heavily on the end user use like SharePoint usage. The end user ensures accuracy of data.

## **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:**

The risk that sensitive PII or sensitive data could be placed in DMAP but not characterized properly.

### **Mitigation:**

The mitigation is that access control is available to those with a need to know based on current access control features. The content owner decides who has access to the content restricting to specifically those who have a need to know.

## **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, the system does have access control levels to ensure that only authorized users view content in the appropriate workspace. EPA information owners/content owners decide which authorized users can access the information in their workspace and that is managed by administrators. As with SharePoint, the user creating the data can restrict who views and edits the data.

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

The EPA DMAP system access control levels, and how content managers can further restrict access is documented within *EPA DMAP Access Controls, Roles and Resource Management*.

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

No, EPA is the only component with 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?**

EPA and credentialed contract support will have access to the data in the system. Contractors with system user access have appropriate FAR clauses included in their respective contracts. The following FAR clauses will be included in the contract:

- 52.224-1: Privacy Act Notification
- 52.224-2: Privacy Act
- 52.224-3: Privacy Training

**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.**

DMAP data is stored and retained according to record schedules associated with programmatic needs and policies dictated by Regulations and Program Requirements.

**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:**

The longer the data is retained the greater the risk of breach, loss, or unintentional destruction from external, internal, and physical risks.

**Mitigation:**

DMAP users will follow programmatic requirements for records retention. The Records Manager and Alternate Records Manager ensure data retention policies and procedures are followed. Controls like encryption and access control restriction limit this exposure. And, the Privacy Officer, Information Security Officer, and Chief Information Officer monitor controls to mitigate any breaches of security and privacy.

## **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.**

Yes. Some information may be shared outside of EPA from DMAP however there is no specific such sharing planned at this time apart from the public facing EPA regulated facility data available from the Envirofacts interface which is fed by the DMAP data warehouse. With agreement from the EPA CISO, there is no PII shared outside of the EPA unless permitted under the statutory authority. It is anticipated that access and use agreements with trusted partners will be established as sensitive data are onboarded to assure that the correct sharing controls are placed on the data. With the example of drinking water data, the anticipation is that these data may need to be shared by the trusted partner data owner with local and state authorities in an emergency response situation. This type of use is already permitted under the statutory authority but permissions will need to be enabled to assure such sharing is possible.

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

DMAP is not a collection system. External sharing is regulated by the source data system.

### **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?**

There is no PII shared outside of the EPA and no external system interconnections unless permitted under statutory authority. An onboarding survey is performed with all newly onboarded data and from this survey it can be determined whether MOUs are required and how access is to be managed. A Change Control Board (CCB) will meet on a biweekly basis to review new uses of data if not already covered under established roles and

permissions, as implemented by DMAP system administrators. Trusted partners will have permissions associated with their roles which will govern their ability to share sensitive data, outside of which new sharing will need to be arbitrated by the CCB.

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

Re-dissemination is restricted or allowed by the individual content owner and in accordance with source system sharing constraints as they pertain to derivative data products from that system.

#### **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 is a risk that PII is accidentally publicly shared.

##### **Mitigation:**

DMAP personnel follow the established processes for managing the sharing of sensitive information. Internal trusted partners receive annual security training around sharing sensitive data. The rest of the data remains internal to EPA requiring a PIV card, encrypted in transit, EPA equipment and single sign on Enterprise Identity Access Management (EIAM) access. Additionally, further restriction of the accessibility is restricted by the content owner.

## **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?**

Auditing and accountability for all data whether public or PII are managed by DMAP system administrators. Accountability is based on the user ID through the EIAM system, which is captured in the logs for auditability.

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

Mandatory EPA Information Security and Privacy Awareness Training occurs on an annual basis.

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

##### **Privacy Risk:**

There is a risk that DMAP user actions cannot be tracked.

### **Mitigation:**

Auditing and accountability occur through application and system level logging significantly lowering the risk.

## **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.**

Information stored in DMAP is available for analytics and data visualization to support the Agency mission.

**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.)*

At a high-level, DMAP is only configured to search for file/app names and streams/controlled shared spaces. The system itself does allow for the retrieval of PII or sensitive data or linkable to an individual (e.g., name and home address) or other data without proper roles and user authorization. However, a credentialed DMAP user may develop views of sensitive data as well as retrieve sensitive data using the sensitive data elements themselves in order to analyze the data for use in supporting the Agency mission.

**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 EPA Information and Content Owner evaluates the probable and potential effect of the privacy of individuals for the PII and sensitive data entered in the DMAP system for this self-service platform. EPA information owners create EPA DMAP information on the EPA DMAP system themselves; EPA information owners specify which authorized users can access those Qlik information; EPA DMAP system owner and EPA DMAP system support staff help EPA information owners to implement controls around the data so that privacy is not invaded and maintain the information in the system of records.

### **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:**

The EIAM single sign on is not used and somehow circumvented.

**Mitigation:**

The DMAP software does not allow this. EIAM as a personal identifier is required to access any content with or without 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.**

The system will provide individuals notice through the publishing of a notice of a new Privacy Act system of records through the Federal Register Online.

**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?**

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

Any individual who wants to know whether this system of records contains a record about him or her, who wants access to his or her record, or who wants to contest the contents of a record, should make a written request to the EPA FOIA Office, Attn: Privacy Act Officer, MC 2822T, 1200 Pennsylvania Avenue NW., Washington, DC 20460.

**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:**

Possibility that individual whose PII is being included has not seen the registry notice.

**Mitigation:**

The registry notice will follow all requirements under the Privacy Act of 1974 (5 U.S.C. 552a) to mitigate any possibility that the initial collection is consistent with the states uses of the information. Additionally, newly onboarded data and users will be surveyed regarding data type and associated restrictions.

## 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.

Each DMAP user can view his or her full user profile within the subsystem within which they have permissions.

### **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.

Users can edit some user data (profile information) whereas as other information (email) may require DMAP help desk support. DMAP help desk can be reached at [dmapadmin@epa.gov](mailto:dmapadmin@epa.gov).

### **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:** There is a risk that someone can impersonate another individual to then submit a privacy act request.

**Mitigation:** EPA follows strict guidelines on processing privacy act requests so will ensure the individual requesting information is indeed intended for that person.