United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev 2/2026 – 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 Roster.docx

System Name: Data Management Analytics Platform (DMAP)		**System Owner: Michael Martinez**	
Preparer: Michael Martinez		**Office:** OFA-SIMD-MOB	
Date: 3/17/26		**Phone:** (202)-566-0797	
Reason for Submittal:			
New: ☐	Revised:☐	Annual Review: x	Rescindment: ☐
System Lifecycle Stage(s):			
Definition: ☐	Development/Acquisition: ☐	Implementation: ☐	
Operation & Maintenance: X	Rescindment/Decommission: ☐		

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:

EPA Data Management Analytics Platform (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.

The DMAP system at EPA is a Cloud data storage analytical platform that provides EPA users with a method to manipulate and analyse data from a multitude of sources. The DMAP system at EPA consists of AWS Cloud based services. This will include the transition of existing AWS Cloud Service (AWS CHS) apps such as ECHO, Tribes and Envirofacts environment under DMAP.

Like Microsoft's SharePoint offering, the DMAP system allows users to maintain control over the workspaces they create and with whom they share their data. The sources for data used by each content user are both internal and external databases and websites.

Section 1. 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) currently exists for DMAP and is regularly updated and maintained in XACTA. A Security Impact Analysis (SIA) will be completed as part of the documentation updates for a Moderate system. ATO expires 11/30/27.

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 an AWS cloud-based service on AWS US Commercial East/West, and is FedRAMP approved. AWS Cloud includes PaaS, IaaS and SaaS offerings.

Section 2. 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 by database storage and stored in Qlik. These data types will be documented in the SSP.

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

- Names
- Phone numbers
- Business Addresses
- E-mail addresses

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

Applications and databases that are onboarded into DMAP will be covered in the DMAP PIA. DMAP users control the data type and method of data input for all data (i.e. scripting or manual processing of excel based spreadsheets/chosen databases). The sources for data used by each created user are both internal and external databases and websites, as well as uploaded documents. DMAP may include scripts and other processes to retrieve the information from either the local/internal data sources or the publicly available information from external databases and web pages.

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, for publicly available data and not for commercial sources. No PII is available through publicly available data unless required by statutory authority.

2.4 Discuss how accuracy of the data is ensured.

Data from Systems of Record is considered immutable for legal purposes and the accuracy of the raw data is not ensured through any automated means as it must be kept intact for record purposes. However, DMAP has automated processes for data cleansing to support analysis, which is done to supplement the original data, however no original data is overwritten. Data in DMAP depends heavily on its data sources and the end users for ensuring 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:

There is a risk that PII could be exposed from DMAP.

Mitigation:

The mitigation is that access control is available to those with a need to know based on current FISMA 800-53 Moderate 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. 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 FISMA 800-53 Moderate 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. 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?

DMAP contains numerous pre-installed access controls (i.e., security rules) documented below:

EPA administrators implement additional access controls/security rules to restrict access to data connections, and which users can view content within streams (i.e., shared spaces).

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?

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 according to programmatic needs and policies dictated by Regulations and Program Requirements. An Electronic Information System Inventory (EISI) form has been completed and submitted on 05/26/2021. DMAP adheres to Schedule 0095 (Web Sites).

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

Mitigation:

DMAP 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. 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 governments, 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.

With agreement from the EPA CISO, there is no PII shared outside of the EPA unless required by statutory authority. The DMAP publishing process will align with EPA standards. The section entitled "External (Public-facing) App Publication (both PII and SPII prohibited)" provides the steps an application owner must follow to publish externally. Application owners are instructed to confer with their privacy official on possible PII and SPII and certify external applications do not contain privacy data. This document is required in order to move an application from the internal development environment to the external public-facing server protecting against PII and sensitive information from being accessed publicly.

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

There is no PII shared outside of the EPA unless required by statutory authority. Only public access information will be shared externally.

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 required by statutory authority. Therefore, no external ISA/MOU are required. If there is an interconnection for whatever reason, then we will follow the given EPA process to create an ISA/MOU.

4.4 Does the agreement place limitations on re-dissemination?

There is no PII re-disseminated outside of the EPA and no external system interconnections unless required by statutory authority. Therefore, no agreements such as ISA/MOU are required. If there is an interconnection for whatever reason, then we will follow the given EPA process to place limitations on re-dissemination.

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 publicly shared.

Mitigation:

DMAP personnel follow the established processes for the posting of publicly accessible information. Approval by the ISO/IMO/SIO for public information with no PII mitigates this risk. The rest of the data remains internal to EPA requiring a PIV card, 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. 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 captured through the DMAP system logs. 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 occur on an annual basis.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Discuss the privacy risks associated with the technical and policy-based safeguards and security measures. How were those risks mitigated?

Privacy Risk:

There is a risk that DMAP actions cannot be tracked for PII upload.

Mitigation:

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

Section 6. 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

List each use (internal and external to the Department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used. If Social Security numbers are collected, state why the SSN is necessary and how it was used.

EPA information owners provide EPA data to the DMAP platform and specify access control levels for their EPA DMAP information. Like SharePoint, the use of each workspace will vary from user to user based on missions and objectives. Not all workspaces will be shared; some are maintained for use only by the individual who created it. The EPA DMAP system makes the information accessible to those EPA users who have been approved by EPA information owners for the access.

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 analyse 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 goal here is to look at the data collected, how you plan to use it, and to ensure that you have limited the access to the people who have a need to know in the performance of their official duties. What controls have you erected around the data, so that privacy is not invaded? ex. administrative control, physical control, technical control.

The EPA Information and Content Owner evaluated the probable and potential effect of the privacy of individuals for the PII entered in the DMAP system for this self-service platform

like SharePoint. 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 platform 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 National Privacy Program (NPP) will determine if a System of Records Notice (SORN) is required. If so, the following additional sections will be required.

Section 7. 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.

DMAP is not an information collection system, it is a data aggregation, warehousing and analysis system. This means that the DMAP does not collect information directly from the individuals, it ingests records/data previously collected. Accordingly, DMAP doesn not present an individual Privacy Act notice at the time of collection. Individuals receive notice from the source systems via Privacy Act Statements when their data is initially collected.

DMAP is covered by SORN: EPA-97. This SORN provides effective notice to the public/individuals in regards to: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary.

Lastly, OFA includes Privacy Act Statements on the account request screen (i.e. the point of collection for account information) and upon login thereafter, to provide additional formal notice to individuals from whom the information is being collected

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?

DMAP is not an information collection system, it is a data aggregation, warehousing and analysis system.

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:

Privacy Risk:

This system does not collect information directly; it aggregates PII from source systems that provide notice at initial collection, and DMAP use is limited to the purposes and routine uses described in those source notices. Privacy Risk: Individuals may not have seen the source registry notice, or registry notice may be unclear.

Mitigation:

DMAP enforces data-sharing agreements and purpose limitation with the source systems and data consumers, minimizes the data used, and masks or excludes records without documented notice or consent.

Section 8. 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.

DMAP aggregates data from other EPA systems and does not provide direct access to edit or manage source records; individuals seeking correction should contact the originating system-of-record in accordance with EPA Privacy Act procedures (40 CFR part 16), and updates at the

source will be reflected in DMAP. DMAP users may view their own account profile within the application based on their role 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.

DMAP aggregates records from authoritative source systems and is not the system of record for collection; individuals seeking correction should submit requests to the originating system in accordance with EPA Privacy Act procedures (40 CFR part 16), identifying the record to be changed and the corrective action sought. Updates made at the source will propagate to DMAP via scheduled synchronization; discrepancies observed in DMAP are routed to the source system owner. Separately, DMAP account/profile information may be edited by users within the application, while certain fields (e.g., email) may require assistance from the DMAP Help Desk at dmap@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 Freedom of Information Act (FOIA).

Privacy Risk:

No privacy risks related to Redress have been identified.

Mitigation:

- Dedicated DMAP Help Desk (dmap@epa.gov) and ticketing for redress requests
- Routing and escalation to source system owners/data stewards; tracking until resolution
- Scheduled synchronization to reflect source corrections; audit logs of changes
- Limited user profile updates supported within DMAP; role-based access controls and oversight by data governance/privacy staff.

I attest as the Agency Privacy Officer that **Data Management Analytics Platform (DMAP)** Privacy Impact Assessment (PIA) has been reviewed. The privacy implications have been adequately identified with appropriate mitigation statements included for implementation in the development or use of information technology systems.

Respectfully,

ROBERT KELLY
Digitally signed by ROBERT KELLY
Date: 2026.05.20 16:04:09 -04'00'

Lee Kelly
Agency Privacy Officer
Cybersecurity Planning & Risk Mgmt Branch
EPA/OFA