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: QLIK	
Preparer: Arthur Zuco**;** Leepchion Linder	**Office:** OMS-OIM-IAASD; OMS/ITSSS
Date: 1/14/2021	**Phone: (**919) 541-4883; (202) 566-2775
Reason for Submittal: New PIA____ Revised PIA_X__ Annual Review____ 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:

EPA Qlik system is a self-service data visualization software platform available to all agency employees as a collaborative shared service. This business intelligence software allows EPA users to transform data into actionable intelligence and automate workflows by connecting to various data sources.

The Qlik system at EPA is a major web-based analytical application that provides EPA users with a method to manipulate and visualize data from a multitude of sources – both internal and external. The Qlik system at EPA consists of an analytics engine, sophisticated artificial intelligence, and web-based frontend/portal where users can create and share "apps" with specific analytical purpose. The Qlik system servers are in the EPA's National Computing Center (NCC) in Morrisville, North Carolina.

Like Microsoft's SharePoint offering, the Qlik 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.

Qlik:

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

Dashboards and visualizations can be shared internally to EPA audiences and to the public per a public approval process. Learn more about Qlik at https://www.qlik.com/us/products/qlik-sense

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) is in progress for the Qlik system and will be placed in XACTA upon completion. A Security Impact Analysis (SIA) was completed in December 2019 and the EPA CIO signed and issued the Qlik Authority to Operate on August 31, 2020 with expiration August 6, 2023.

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, the data will not be stored in the cloud. Qlik isn't a cloud system.

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 by user-created Qlik apps and stored in Qlik user workspaces. These data types will be documented in the SSP.

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

- Names
- Phone numbers
- Business Addresses
- E-mail addresses
- Human resource records including DOB, salary, employee ID, race (Hispanic or not), ethnicity (Caucasian, Asian), disability status, and veteran status. It does not include SSN, Name, Physical or mailing address, or emails. The employee ID is the de-identifier
- Employment histories
- Salary histories
- Personal info: schedules, habits, interests, travel histories, planned vacations, articles written, professional society memberships.

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

Applications that are onboarded into QLIK will be covered in the QLIK PIA. Qlik 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 app are both internal and external databases and websites, as well as uploaded documents. Qlik user apps are scripted 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 no 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.

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 could be placed on Qlik.

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. 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?

Qlik contains numerous preinstalled access controls (i.e., security rules) documented below:

ManagementConsole/Content/Sense_QMC/preinstalled-QMC-security-rules.htm

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 Qlik system access control levels, and how content managers can further restrict access is documented within ***EPA Qlik 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.

Based on EPA scheduled number 1012, the EPA Qlik information is retained online for 365 days.

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:

Qlik follows record retention schedule 1012. 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.

With agreement from the EPA CISO, there is no PII shared outside of the EPA unless required by statutory authority. The Qlik publishing process is described at this website https://dmaponline.epa.gov/qlik_production.html. The section entitled "External (Public-facing) App Publication (both PII and SPII prohibited)" provides the steps an application owner must follow to publish externally. Central to the external publication process is the Qlik PII questionnaire. 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 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 shared outside of the EPA and no external system interconnections unless required by statutory authority. Therefore, no 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:

Qlik 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 5.0 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 captured through the Qlik application and 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 occurs on an annual basis.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

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

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.

EPA information owners create EPA Qlik information and specify access control levels for their EPA Qlik 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 Qlik 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__ 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.)

At a high-level, Qlik is only configured to search for file/app names and streams/controlled shared spaces. The system itself does not allow for the retrieval of PII linked or linkable to an individual.

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 entered in the Qlik Application for this self-service platform like SharePoint. EPA information owners create EPA Qlik information on the EPA Qlik system themselves; EPA information owners specify which authorized users can access those Qlik information; EPA Qlik system owner and EPA Qlik 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 Qlik application 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.

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?

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:

Mitigation:

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?

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

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:

Mitigation: