United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 1/2020)
(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.
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf. If you need further assistance, contact your LPO.

System Name: Viper	
Preparer: Joe Schaefer	**Office: OLEM/OSRTI/TIFSD/ERT**
Date: 2/5/2020	**Phone: 609-865-8111**
Reason for Submittal: New PIA__X__ Revised PIA____ 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:

Viper is designed to capture data streams from an instrument, used to collect monitoring data, and delivers the data to a web site in near real-time. Instrument monitoring uses specific sensors that are appropriate for the sampling event. The sensors stream the data and Viper Survey Controller captures the data and transmits it to Viper Deployment Manager. Alarms and alerts can be configured and users can be notified of any exceedances of monitoring thresholds. Users can also view the data streams in near real-time and determine if the there is a need for action.

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?

CERCLA: 42 U.S. Code 9604 Response Authorities (b)(1)

(b) Investigations, monitoring, coordination, etc., by President

(1) Information; studies and investigations

Whenever the President is authorized to act pursuant to subsection (a) of this section, or whenever the President has reason to believe that a release has occurred or is about to occur, or that illness, disease, or complaints thereof may be attributable to exposure to a hazardous substance, pollutant, or contaminant and that a release may have occurred or be occurring, he may undertake such investigations, monitoring, surveys, testing, and other information gathering as he may deem necessary or appropriate to identify the existence and extent of the release or threat thereof, the source and nature of the hazardous substances, pollutants or contaminants involved, and the extent of danger to the public health or welfare or to the environment. In addition, the President may undertake such planning, legal, fiscal, economic, engineering, architectural, and other studies or investigations as he may deem necessary or appropriate to plan and direct response actions, to recover the costs thereof, and to enforce the provisions of this chapter.

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?

Yes. Yes, the system has an ATO. The ATO expires on 4/19/2022.

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?

Yes, the system is hosted at AWS in their FedCloud which has gone through the FedRAMP certification process. It is procured through an IA with DOI to provide EPA IaaS for systems related to emergency response.

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).

The system stores information predominantly related to sensor data so things like parameter, result, units, date/time, sensor ID, and data elements that allow you to group the sensor data for example, user defined identifications for the project name and a sequential run identification.

Name, Business Phone Number, Business Email address are the PII elements and are related to the user account info.

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

The source is sensor data coming directly from deployed field instruments (GFE) after it undergoes a translation process to convert data into the proper format for Viper ingestion. Viper then transmits the data livestream to a web site for viewing.

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.

Integrity of the data is maintained due to secure SSH wireless electronic transmissions. The Viper system does not ensure accuracy of the data as it is supplied by the instrumentation's sensor readings and the system cannot verify sampling data.

The sensor data stored by Viper is coming from instrumentation that is being deployed according to a site-specific quality assurance project plan. That QAPP should dictate how the instrument is to be calibrated.

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 low risk of inaccurate information due to human error.

Mitigation:

User's verify their information prior to account creation.

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?

Users of the Viper Deployment Manager web site are required to register in order to gain view only access to specific deployments to which they have been granted privileges. Data can only be viewed in deployment manager. The privileges are granted by the site OSC through response.epa.gov web site Contact Manager.

3.2 What procedures are in place to determine which users may access the information and how does the system determine who has access?

The Viper System Security Plan (SSP) and Account Management Plan details the procedures for user access and controls.

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

There are administrators of the Viper Deployment Manager and these privileges are approved and assigned by the System Owner. Administrators of the web site allows users to create deployments, assign monitoring events to deployments, and manage alarms and notifications.

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 from General Dynamics Information Technology (GDIT) have administrative access to the system. Yes, the FAR clauses are included in the contract.

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.

Viper System would fall under the Superfund record schedule EPA Records Schedule 1036. Records kept under record schedule 1036 are kept for 30 years and then they are destroyed. These records are kept in order to ensure that EPA is following the guidelines set forth by the

National Archives and Records Administration.

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:

Information may be retained longer than it is needed.

Mitigation:

The appropriate record control schedule is properly followed.

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.

Viper monitoring data is not shared with non-EPA partners. On a site by site basis, the Federal On-Scene Coordinator or Remedial Project Manager may allow access to non-EPA personnel. This is following the Regional practices they use to work with site stakeholders and enable access to information on the site.

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

EPA SORN 74 states that "Records may also be disclosed to public health authorities in conformity with federal, state, and local laws when necessary to protect the public health or safety, or to federal, state, or local governmental agencies when it is determined that a response by that agency is more appropriate than a response by the EPA"

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?

That is the responsibility of the Region and the site project manager (OSC or

RPM)

4.4 Does the agreement place limitations on re-dissemination?

No.

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 minimal risk of potential exposure to PII. The information could potentially be shared with someone who did not need access to the information.

Mitigation:

Access to the system is role based. There is a user agreement in place instructing users to adhere to the rules of behavior.

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?

Access to the system requires a secure user account that adheres to the SSP account controls in accordance with NIST SP 800-53 Rev 4. Administrators have signed ROB for the system.

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

Administrators are provided the Viper Admin User Guide. Administrators also take the annual required Security and Privacy Awareness trainings provided by the EPA and General Dynamics.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

There is a minimal risk of potential exposure to PII.

Mitigation:

PII is limited to what is business related information, as part of the user self-registration process. Users have to change their passwords every 60 days which give them the opportunity to review their information for accuracy.

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.

Viper live-streams the sensor data it collects and displays it in a graphical format to enable decision making by project managers (EPA personnel i.e. OSCs) via the Viper Deployment Manager web site. Examples of decisions may include evacuation based on Action levels defined by the EPA based on the contaminant. The users can only View the data. Alarms can be enabled to alert response personnel about action level warnings or exceedances via text or emails based on Action levels.

Deployments are controlled by security level with the site owner managing access for the users via a corresponding response.epa.gov site. The site manager is making the determination on who should have access to what information based on the real-world needs of the project. This mimics how that site manager is distributing all other information related to the cleanup project be it email distribution, conference call participation etc

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.)

The Viper system is designed to retrieve monitoring data sets by selecting a deployment name which typically corresponds to a superfund site name. Within a deployment (site or areas where monitoring is equipment is deployed), users can retrieve data by selecting a specific instrument. Monitoring equipment may be fixed or mobile. No PII is retrieved or displayed during any of the process.

6.3 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

If the site deals with a residential cleanup, EPA SORN 74 – Environmental Assessment of Residential Properties may apply, but there are no designated fields to associate the sensor data with any residential property identifiers used during other aspects of the environmental assessment and clean up so the associations are usually managed outside of the system (i.e. site log books).

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 risk is potential unauthorized use of information.

Mitigation:

PII is verified through the account creation to ensure that PII is only used for the purpose of collection.

*If no SORN is required, STOP HERE.

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: