

## PRIVACY IMPACT ASSESSMENT

(Rev. 04/2019)

(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official

[http://intranet.epa.gov/privacy/pdf/lpo\\_roster.pdf](http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf). If you need further assistance, contact your LPO.

<b>System Name: Scribe.NET</b>		
<b>Preparer: Joe Schaefer</b>	<b>Office: 2890 Woodbridge Ave, Edison, NJ 08837</b>	
<b>Date: 2/27/2020</b>	<b>Phone: 732-906-6920</b>	
<b>Reason for Submittal: New PIA</b> ____ <b>Revised PIA</b> ____ <b>Annual Review</b> __ <u>X</u> __ <b>Rescindment</b> ____		
<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"/>		
<p><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></p> <p><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></p>		

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

Scribe.NET is a web-based centralized repository for Scribe project databases of field sampling information collected in Scribe. Residential sampling events may contain PII of residents such as Name, address and phone number. Scribe.Net has limited used by system administrators only and accessible only with a secure login. The Scribe.NET ingests and versions individual Scribe project databases and has the capability of aggregating individual Scribe project databases into one large database. Users are administrators of the system and interface with Scribe.NET only through the Scribe desktop application utilizing subscription service accounts specific to each project database. Discrete database service connections can be established to Scribe.NET for regularly subscribed information and requires a secure non-interactive service account over Secure Socket Shell (SSH). Projects are optionally published to Scribe.NET and available to users by subscription only. A subscription (if necessary) is created for a particular project or a combination of projects by the administrators of the system. The secure subscription information is provided to the project owner and they are responsible for providing that information to the users they deem necessary.

## **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, the system has an ATO. The ATO expires on 6/02/2022

### **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 data is maintained in FedRAMP approved AWS cloud. The service provider delivers IaaS.

## **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).**

System accounts include Last Name, First Name, Business Address, Business Phone numbers and Business email addresses. In the cases of residential sampling, Scribe.NET manages individual Scribe projects and may contain residential sampling data that contains the types of data collected in environmental assessments including names of residents; address information; phone number or other contact information.

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

The sources are individual Scribe project databases of field sampling events that are published to Scribe.NET system. The data is field sampling data collected via various types of media and monitoring. The OSC and their application administrators provide the site and lab information. The act of publishing sends a complete copy of the Scribe database to the Scribe.NET system where it is compared to previously published versions and changes, additions and deletions are captured. The EPA Computer Warning Banner about privacy is displayed on the register/login page.

### **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. The field sampling data is stored and sometimes aggregated into larger databases for analysis and evaluating clean-up or remediation decisions.

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

Integrity of the data is maintained due to electronic transmissions via SSH only and project owners are exclusive for each project using username and machine IDs. The system does not ensure accuracy of the data as it is supplied by the users and the system cannot verify sampling 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 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 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.

Only Scribe.NET administrators (EPA Project officer and designated EPA contractors with privileged rights) have access to Scribe.NET user information. Administrators are administrators of the system and follow the Scribe.NET ROB. Administrators require a username and login that comply with Scribe.NET SSP user account controls.

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

Only Scribe.NET administrators (EPA Project officer and designated EPA contractors with privileged rights) have access to Scribe.NET user information. Administrators are administrators of the system and follow the Scribe.NET ROB. Administrators require a username and login that comply with Scribe.NET SSP user account controls. Controls are documented in the Scribe.NET SSP and Rules of Behavior signed annually by administrators.

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

No.

### **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.**

Scribe.NET would fall under the Superfund record schedule EPA Records Schedule 1036. Records are retained for possible lawsuits against a company for illegal environmental activities and will be retained for at least 2 years after the data is no longer needed.

**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 could be maintained longer than needed.

**Mitigation:**

The system follows the Superfund records schedule.

## **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.**

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 in accordance with stated practices in this PIA (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 Scribe.NET 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 low risk that improper log audit may lead to unaccounted data.

**Mitigation:**

Audit logs are frequently reviewed.

## **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 Scribe.NET system facilitates the receipt and repository of Scribe database projects of field sampling information from national response activities. Allows the EPA's Emergency Response program to improve operational effectiveness, reduce costs, streamline business processes, and enhance information management capabilities.

The Scribe.Net system enables data warehousing of electronic records of sampling data and marry them with lab results. This allows for annotation of EPA's evaluation in response to removal and remedial sites. The application addresses the growing demands of content management, data exchange, geospatial visualization and analytical processing.

### **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 system is designed to retrieve projects by Publisher Region and ProjectID.

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

Scribe.NET manages the publishing and distribution of Scribe datasets. A Scribe project that is published to Scribe.NET may be used to document the sampling and analytical data related to a residential cleanup. That data would fall under EPA SORN 74 – Environmental Assessment of Residential Properties.

### **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.**

*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 How does the system notify individuals about the procedures for correcting their information?**

**8.4 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:**