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:** Stratospheric Protection Division System (SPDS) | |
| **Preparer:** Patrick Lau and John Kahanek IV | **Office:** OAR/OAP/SPD |
| **Date:** 09/13/2023 | **Phone:** 202-564-7312 and 832-432-7773 |
| **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 ☐<br>**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).**<br>**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:

Stratospheric Protection Division System (SPDS), hosted in a FedRAMP Moderate PaaS CSP, is a multi-year project to develop a new reporting and database system and modernize existing applications that will manage all aspects of the collection, maintenance, and dissemination of EPA's programmatic data. This includes allowance trading, compliance, company, contact, program, and regulatory agency data pertaining to ozone depleting substance (ODS) and hydrofluorocarbon (HFC) programs administered by EPA.

The data to be collected in SPDS are and will be from EPA Regulatory Programs that include the American Innovation and Manufacturing (AIM) Act, Title VI and Section 608 of the Clean Air Act, Significant New Alternative Policy (SNAP) Program: and other voluntary programs such as GreenChill and Responsible

Appliance Disposal (RAD), all administered by EPA.  Some of the data is considered confidential business information (CBI).

Phase I will begin with the development of a regulatory reporting application that must be in production by June 2024 to meet our statutory reporting deadlines. The application is a data collection tool that will collect regulatory data and disseminate machine-readable identifiers and will require authentication and CROMERR.

The SPDS receives the following personally identifiable information (PII) from CDX, which in most cases is available company data:

- Individual Name
- Company Name
- Company Email Address
- Company Address
- Company Phone Number

## 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?

This plan was developed in response to the requirements of the following laws and regulations:

- 42 U.S.C. §7675 - American Innovation and Manufacturing (AIM) Act of 2020.  The AIM Act authorizes EPA to address hydrofluorocarbons (HFCs) by providing new authorities in three main areas: to phase down the production and consumption of listed HFCs, manage these HFCs and their substitutes, and facilitate the transition to next-generation technologies through sector-based restrictions.
- 40 C.F.R. 84 - Phasedown of Hydrofluorocarbons. The Act mandates the phasedown of hydrofluorocarbons (HFCs), which are highly potent greenhouse gases (GHGs), by 85 percent by 2036.
- 44 U.S.C. § 3506, which establishes federal agencies' responsibilities for managing information resources and 40 U.S.C. § 11315, which establishes the responsibilities of the agency's Chief Information Officer to manage agency information resources.
- The Title of the E-Government Act of 2002 - Federal Information Security Management Act (FISMA) – Public Law 107-347: A security plan must be developed and practiced throughout all life cycles of the agency's information systems.
- Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources: A System Security Plan (SSP) is to be developed and documented for each GSS and Major Application (MA) consistent with guidance issued by the National Institute of Standards and Technology (NIST).
- Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems: This document defines standards for the security categorization of information and information systems. System security categorization must be included in SSPs.
- FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems: This document contains information regarding specifications for minimum security control

requirements for federal information and information systems. Minimum security controls must be documented in SSPs.
- NIST Special Publication (SP) 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems: The minimum standards for an SSP are provided in this NIST document.
- NIST SP 800-53, Revision 4, Recommended Security Controls for Federal Information Systems and Organizations: This document contains a list of security controls that are to be implemented into federal information systems based on their FIPS 199 categorization. This document is used in conjunction with FIPS 200 to define minimum security controls, which must be documented in SSPs.
- EPA Information Security Planning Policy. A system security plan shall be developed for each system cited on the EPA Inventory of Major Information Systems, including major applications and general support 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 in XACTA will be completed once it is in XACTA.
- The system will have an ATO by June 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.

The OMB Control # is 2060-0734. The EPA ICR # is 2685.02.

### 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?

- The data will be stored in the cloud.
- The cloud.gov provider is FedRAMP Moderate.
- The type of service from the CSP is a Platform as a Service (PaaS).

## 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).

User Registration Data: To access SPDS, users must first register as users with CDX by providing identifying information including:

- Individual Name
- Company Name
- Company Email Address
- Company Address

- Company Phone Number

Users may also be required to complete an Electronic Signature Agreement (ESA). The information will then be passed onto SPDS and used for registration, identify the information the registered user collects, and for general communication and accountability with the user.

AIM Data: Users can submit data reports on production, import, export, transformation, destruction, and reclamation of chemicals regulated under AIM. The complete list of data elements collected can be found under 40 CFR Part 84.

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

CDX collects the following information inputted by the user through a registration process and passes over to SPDS.

- Individual Name
- Company Name
- Company Email Address
- Company Address
- Company Phone Number

AIM data can be entered by any of the individuals registered with their specific company.

### 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 PII is collected during the registration process by the user via CDX.

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

The PII related information is inputted by the user during the registration process. **Additionally, CDX** will have some additional checks for verification and validation including individual verification.

- Individual Name
- Company Name
- Company Email Address
- Company Address
- Company Phone Number

### 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:**

Data elements collected by CDX and passed to SPDS follows.

1. Individual Name

a. Risk that individual name could be taken in an unauthorized manner.

2. Company Name

   a. No known risk as the company name is publicly listed.

3. Company Email Address

   a. Risk that email address may contain the user's name.

4. Company Address

   a. No known risk as the company address is publicly listed.

5. Company Phone Number

   a. No known risk as the company phone number is publicly listed.

**Mitigation:**

Role and permission-based access will be in use to restrict access to those who have a need to access this information. Additionally, the data will reside in the AWS Relation Database Service (RDS) Postgres Database, which is encrypted for data-at-rest using AES 256 bit. Data-in-transit will also be encrypted with SSL.

## 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. Role and permissions-based access control will be used to prevent accessing information that the users do not have permission to access. All access controls will be documented in the System Security Plan (SSP).

Without a user account in CDX, the user will not be able to access the system. All other access requires authentication. Following authentication, access to data requires the proper permission/roles as described below (i.e. access to data is role-based).

The default role is the "preparer" role. This is the role used to submit data for their company. Note that, more than one individual can access data for the same company. In that case, the Company Representative is responsible for determining which Alternative Company Representative or Agent(s) can access the company data.

EPA and EPA contractor users may receive the "Data Analyst" role that provide access the data submitted by the companies. EPA and EPA contactors may also be given the "Help Desk" role.

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

The Access Management Procedure (AMP) and System Security Plan (SSP) identifies the roles and permissions as well as how access is granted, modified, and terminated.

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

Other roles outside of our purview for the layers below the application like the database, operating system, and network layer are owned by the CSP.

### 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?

Federal employees as well as contractors will have access. External Reporters will have access to only the data that the submit. Yes, the appropriate 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.

SPDS will retain data as required and specified by the following 2 acts:

- 42 U.S.C. §7675 - American Innovation and Manufacturing (AIM) Act of 2020. The AIM Act authorizes EPA to address hydrofluorocarbons (HFCs) by providing new authorities in three main areas: to phase down the production and consumption of listed HFCs, manage these HFCs and their substitutes, and facilitate the transition to next-generation technologies through sector-based restrictions.
- 40 C.F.R. 84 - Phasedown of Hydrofluorocarbons. The Act mandates the phasedown of hydrofluorocarbons (HFCs), which are highly potent greenhouse gases (GHGs), by 85 percent by 2036.

Otherwise, we intend to follow EPA data retention policy.

### 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:**

Minimal risk as the data will have access restricted based on role and permission based access to those who have a need to access this information. Additionally, the data will reside in the AWS Relation Database Service (RDS) Postgres Database, which is encrypted for data-at-rest using AES 256 bit. Data-in-transit will also be encrypted with SSL.

**Mitigation:**

Role and permission-based access will be in use to restrict access to those who have a need to access this information. Additionally, the data will reside in the AWS Relation Database Service (RDS) Postgres Database, which is encrypted for data-at-rest using AES 256 bit. Data-in-transit will also be encrypted with SSL.

## 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.

No reports are scheduled to be produced for information sharing. In the future, non-CUI data may be provided to the public. The data may contain information related to a company’s activities. No data related to individuals will be released to the public or shared outside of EPA.

Reporters may be able to access and download data they submitted on behalf of their company. Company Representative and the Alternate Company Representative may be able to display a list of users associated with their company.

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

No reports are scheduled to be produced for information sharing. In the future, non-CUI data may be provided to the public in accordance with the AIM Act.

### 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?**

EPA does not have information sharing agreements or MOUs and does not grant access to the system by organizations outside of EPA.

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

EPA does not share or publish ANY data related to individuals (PII).

### 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:**

None – No external or internal agencies, state or local government will have access to the data contained within the AWS Relation Database Service (RDS) Postgres Database, which is encrypted for data-at-rest using AES 256 bit.

**Mitigation:**

None

## 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?

There are SOPs that will regulate the use of information gathered and used in the AWS System. Access to application deployment and application-level logs will be accessible by the application EPA SPDS team. Other logs below the application including the database, operating system and network layer will be accessible by the CSP. We intend to forward the application-based logs to EPA Splunk, which exceeds a 2-year retention.

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

All users of the system must read, acknowledge, and adhere to the system Rules of Behavior.

All EPA and EPA contractor users are required to take mandatory Annual EPA Information Security and Privacy training per the EPA Privacy Policy and the EPA Information Security Policy.

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

**Privacy Risk:**

Minimal. Auditing and accountability occur through logging in AWS Relation Database Service (RDS) Postgres Database and is handled by the CSP.

**Mitigation:**

Auditing and accountability occur through logging in AWS Relation Database Service (RDS) Postgres Database and is handled by the CSP.

## 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 system uses user registration data to allow the user to access the system. The information will then be used to identify data submitted by the user, and for communication and accountability with the user.

AIM Data is required to be reported under 40 CFR Part 84.: Users can submit data reports on production, import, export, transformation, destruction, and reclamation of chemicals regulated under AIM. The complete list of data elements collected can be found under 40 CFR Part 84.

### 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 sort information by Company Name for retrieval.

### 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 probability or potential effect of the privacy of personally identifiable information (PII) will be low with the totality of SSP controls. Specifically, the following controls make the chance of loss of privacy low.

- Search will occur based on company name as an identifier.
- Role and permission-based access will be in use to restrict access to those who have a need to access this information.
- The data will reside in the AWS Relation Database Service (RDS) Postgres Database, which is encrypted for data-at-rest using AES 256 bit. Data-in-transit will also be encrypted with SSL.

### 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:**

Minimal. Search will occur based on company name as an identifier.

**Mitigation:**

Mitigation occurs for privacy based on the following controls.

- Search will occur based on company name as an identifier.
- Role and permission based access will be in use to restrict access to those who have a need to access this information.
- The data will reside in the AWS Relation Database Service (RDS) Postgres Database, which is encrypted for data-at-rest using AES 256 bit. Data-in-transit will also be encrypted with SSL.

*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.

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.

### 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?

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.

### 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.

### 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: N / A**

**Mitigation: N/A**