

# 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](https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx)

<b>System Name: System for Risk Management Plans (SRMP)</b>	<b>System Owner: Mark Douglas</b>
<b>Preparer: Mark Douglas</b>	<b>Office: EPA/OLEM/OEM</b>
<b>Date: 4/16/2021</b>	<b>Phone: 202-556-5572</b>
<b>Reason for Submittal: New PIA</b> <input type="checkbox"/> <b>Revised PIA</b> <input type="checkbox"/> <b>Annual Review</b> <input checked="" type="checkbox"/> <b>Rescindment</b> <input type="checkbox"/>	
<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"/>	
<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>	
<b>The PIA must describe the risk associated with that action. For assistance in applying privacy risk see <u><a href="#">OMB Circular No. A-123, Section VII (A) (pgs. 44-45).</a></u></b>	

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

The purpose of the System for Risk Management Plans (SRMP) is to provide EPA with a mechanism for collecting Risk Management Plans (RMP) from regulated facilities to:

- Ensure that submissions are error-free;
- Provide RMP database information to “covered persons” and approved nodes in federal, state, and local government;
- Provide query and analysis capability to the user community.

A critical aspect in all these functions is the safeguarding of Offsite Consequence Analysis (OCA) information. OCA consists of sections of the RMP which contain information that Congress has instructed

EPA to safeguard and make available only to covered persons. (Definition: Chemical Safety Information, Site Security and Fuels Regulatory Relief Act (CSISSFRRRA) applies its restrictions to covered persons. The OCA regulations use the term “government officials” to refer to the largest categories of covered persons. The three categories of covered persons are: federal government officials, state/local government officials, covered researchers.)

SRMP is hosted in the Central Data Exchange (CDX) environment. The CDX environment contains the following data: name of individual system user, self-assigned user name; security password, verification questions, work address, work contact information (e.g., phone and fax numbers, email address), and user’s EPA Program ID and role related to electronically filed reports.

The CDX registration system is in an encrypted database that is inaccessible to administrators and users. CDX stores user’s self-assigned password created during registration. CDX stores other system-generated data such as the registration date and time, digital certificate identifier, and identifiers used for internal tracking. CDX does not create specific personal identifiers for registrants.

## **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?**

Section 112(r) of the Clean Air Act Amendments requires EPA to publish regulations and guidance for chemical accident prevention at facilities that use certain hazardous substances. These regulations and guidance are contained in the Risk Management Plan (RMP) rule. The information required from facilities under RMP helps local fire, police, and emergency response personnel prepare for and respond to chemical emergencies. The RMP rule was built upon existing industry codes and standards. It requires facilities that use listed regulated Toxic or Flammable Substances for Accidental Release Prevention to develop an RMP and submit that plan to EPA.

### **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. Both CDX and SRMP have System Security Plans. Yes, the system has an ATO that is set to expire on 10/30/2023.

### **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.**

Yes, OMB Control Number: The RMP\*eSubmit User’s Manual includes the Risk Management Plan Form and other forms as appendices. These forms include OMB Control Number: 2050-0144. Agency Number: Risk Management Plan Form: EPA Form 8700-25;

**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. Microsoft Azure Commercial and Government cloud services are used within CDX. Both are FedRAMP approved and used for PaaS and 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).**

SRMP enables chemical facilities to enter data through a system that will allow them to electronically prepare a Risk Management Plan (RMP). There are nine sections in an RMP:

- Registration Information
- Sections 2-5 Offsite Consequence Analysis (OCA) Information – In these sections, facilities define worst case and alternative release scenarios about potential releases of toxic and flammable substances.
- Section 6 Five Year Accident History – Facilities report accidents that have occurred within the last five years involving regulated substances held above the threshold quantity.
- Sections 7-8 Prevention Programs for Program Level 2 and 3 Processes – Facilities define the policies, procedures, mechanisms, and training programs that are implemented to help prevent accidents.
- Section 9 Emergency Response Plan – Facilities describe the facility plan for responding to emergencies.

In order for a facility to submit an RMP it must first submit, and receive approval for, an Electronic Signature Agreement (ESA) for the facility. The ESA links a Certifying Official to the facility. (Definition: Certifying Officials are facility owners or operators who must certify the accuracy and completeness of the information reported in the RMP.) When a Certifying Official's ESA is approved, the Certifying Official receives an email with an authorization code that will be passed to the RMP Preparer for use in registering for a Prepare Submission role. (Definition: Preparers are facility representatives, granted permission by a facility to access the facility's existing RMP. They prepare data for a new or updated RMP.)

RMP Reporting Center personnel also enter information into the system to manage user accounts for RMP\*Info, RMP Download Dataset, and RMP\*eSubmit.

•For RMP\*Info users this information includes the User Name, Work Phone Number, Organization, and State. An account number is also assigned to each user.

•For RMP Download Dataset users this information includes the User Name, Work Phone Number, Organization, and State. An account number is also assigned to each user.

When the RMP Reporting Center receives correspondence from a facility, a record is created in the Tracking System with the name of the user, the name of the facility, and the address of the facility.

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

Primary source of information is from the regulated community (facilities). This information is collected via online submissions (>99%) and through paper form submissions (<1%).

## **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.**

There are multiple validations. Certain fields are restricted by values / ranges of values. For example, fields may be validated against a reference table. Latitude / Longitude are validated against a county bounding box. A value of a field may be based upon the value entered in another field. Certifying Officials are only allowed to submit their RMP once all data validations have been successfully passed.

## **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:**

Security categorization of the system was determined based on the following:

- The risk of loss of confidentiality of the RMP information is low because RMP information is disseminated to the public via controlled mechanisms (e.g., Federal Reading Rooms, LEPCs, and facilities). Therefore, the loss of confidentiality of RMP information would have limited adverse impact on the organizational operation, organizational assets, or individuals.
- The risk of loss of integrity is medium because serious adverse impacts on emergency response and the reputation of OLEM could be incurred from the dissemination of incorrect/corrupted information.
- The risk of loss of availability of the system is low because facilities can submit on paper forms during an outage, the RMP Reporting Center can distribute existing copies of the database on DVD for analysis, and alternate RMP processing sites exist. Therefore, the loss of availability of the RMP applications hosted in CDX would have limited adverse impacts on organizational operations, organizational assets, or individuals.

### **Mitigation:**

SRMP undergoes an annual Risk Assessment as part of a continuous monitoring cycle which requires that 1/3 of the security controls be reviewed each year. The RA & CM is conducted by a third-party assessor. The last SRMP RA & CM was conducted in April 2017.

## **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?**

Within CDX user access to RMP information is controlled through the use of CDX roles. Authorized Preparers and Certifying Officials are assigned roles. These roles allow them access to their own RMP(s). RMP\*Info, RMP\*Download Dataset, RC Management, and RMP Reporting Center (RMP RC) Staff are all closed registration applications. Users contact the RMP RC to request access. The RMP RC contacts EPA about the requests and grants access only after the requests are approved by EPA. Additional restrictions (e.g., access by state) may apply within each application.

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

As part of registering with CDX users may add a Certify Submission role to their account and submit an Electronic Signature Agreement (ESA) for one or more facilities. Upon verification that an ESA submitter is an authorized representative for the designated facilities, the EPA Facility ID of each facility is linked to the requestor's Certify Submission role. The Certifying Official is also provided with an authorization key that may be used to register for a Prepare Submission role for the purpose of preparing an RMP.

Requests to access to all other RMP functions within CDX must be sent to the RMP Reporting Center and approved by EPA. After approval, the appropriate CDX role is assigned by the RMP Reporting Center. Additional access settings may also be configured.

### **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?**

Both Agency and Agency contractor employees have access to the data/information on CDX. The appropriate clauses have been incorporated into the contract and provide a foundation for the contractor's privacy data protection policies. These clauses are the Federal Acquisition Regulations (FAR) clauses (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act).

### **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.**

EPA Records Schedule 0047.

The information from the schedule is below. To clarify, RMP permanently maintains all submitted data in the database. The original requirement was to maintain the data in system for 10 years. However, with advances in storage systems which increased availability and reduced costs for storage, EPA decided data should be maintained indefinitely for emergency response and preparation purposes. The schedule also refers to how long NARA maintains copies of the data.

### Disposition Instructions:

Item a: (Reserved)

Item b: (Reserved)

Item c: RMP\*Administration electronic data

NARA Disposal Authority: N1-412-05-2c

- Permanent
- Close file when program discontinued or no longer needed for current agency business, whichever is longer.
- Transfer the data to the National Archives after file closure, as specified in 36 CFR 1235.44-1235.50 or standards applicable at the time.

Item d: (Reserved)

Item e: (Reserved)

Item f: (Reserved)

Item g: All other electronic data NARA Disposal Authority: N1-412-05-2g

- Disposable
- Close file when superseded.
- Delete after file closure.

Item h: (Reserved)

Item i: (Reserved)

### Guidance:

Media neutral - This schedule authorizes the disposition of the record copy in any media (media neutral). However, if the format (e.g., electronic) of permanent records is specified in a records schedule approved by NARA, the records are to be transferred to the National Archives in accordance with NARA standards at the time of transfer. If the record copy is created in electronic format or digitized (e.g., imaged) and maintained electronically (e.g., Data on Aquatic Resources Tracking for Effective Regulation (DARTER) maintained in the Office of Water), the electronic records must be retrievable and usable for as long as needed to conduct Agency business and to meet NARA-approved disposition to comply with 36 CFR Sections 1236.10, 1236.12, 1236.14, and 1236.20. Retention and disposition requirements for the various components of electronic systems (e.g., software, input, output, system documentation) are covered in schedule 1012, Information and Technology Management. In addition to 36 CFR 1236, see "Basic Requirements of an Electronic Recordkeeping System at EPA" on the EPA records intranet site <http://intranet.epa.gov/records/tools/erks.html>.

Sensitive information - When records are due for destruction according to the disposition

instructions, records containing sensitive information (e.g., confidential business information (CBI), personally identifiable information (PII), offsite consequence analysis (OCA)) must be shredded or otherwise definitively destroyed to protect confidentiality.

OLEM headquarters, through the RMP Reporting Center, is responsible for the original RMPs that were submitted on disk/diskette or in paper format and data in the CDX, as well as the record copy of all software and software documentation. The implementing agencies will manage the records they use for implementing the program, etc. The original RMPs which may have been submitted by facilities and the RMP implementation-related records managed by the implementing agencies are all covered by schedule 1035, item c. By default, EPA regions are the RMP implementing agencies.

States can choose to take delegation of this program, and if so, they become the implementing agency. If the state is the implementing agency, they are responsible for the program records. Records related to EPA oversight of the state program are covered by schedule 1016, item c.

Electronic software program - The electronic software program, formerly item a, is to be kept as long as needed to ensure access to, and use of, the electronic records throughout the authorized retention period to comply with 36 CFR Sections 1236.10, 1236.12, 1236.14, and 1236.20. NARA regulations require that electronic records be retrievable and usable for as long as needed to conduct agency business and to meet NARA-approved disposition, and is covered by schedule 1012, item e.

Input - Input, formerly item b, is covered by schedule 1012, item e.

RMP\*Administration - Item c for RMP\*Administration includes the Executive Summary (formerly RMP\*Maintain Executive Summary), the electronic data (formerly item d), RMP\*Maintain data), and the graphics (formerly item e, RMP\*Maintain Graphics). Data formerly contained in RMP\*Maintain has been migrated to the RMP database that is currently in use.

RMP\*Review audit and user-defined data - Recipients of the data can use RMP\*ReviewAdmin to enter audit and user-defined data, formerly item f, into their databases and are therefore responsible for the management of it.

Output and reports - For disposition of output and reports, formerly item h, refer to the records schedule for the activity supported by the output and reports. Follow the disposition instructions for the applicable records schedule item. If more than one records schedule or item applies, follow the disposition instructions with the later date.

System documentation - Supporting or system documentation, including system development documentation, formerly item i, refers to those records necessary to document how the system captures, manipulates and outputs data. System documentation is transferred to the National Archives along with the electronic data. Disposition of system documentation is covered by schedule 1012, item a.

Related schedules - The CDX is covered by schedule 0097.

### 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:**

Risks evaluated:

- Laws and regulations are violated as a result of lack of controls over collection of personally identifiable information (PII).
- Laws and regulations are violated due to data not being retained for the required duration of time or due to inappropriate data being stored.
- Laws and regulations are violated as a result of lack of controls over use of personally identifiable information (PII) in testing, training and research.

Since RMP information is made available to the public and may exist in the public domain without restriction, there are no risks related to the retention of the information.

#### **Mitigation:**

Any privacy risks identified in this system are mitigated by the security and privacy controls implemented in the SRMP SSP under 14.22 - DATA QUALITY AND INTEGRITY (DM).

Mitigation considered:

- A privacy impact assessment determines the extent and nature of PII in the organization, and appropriate handling mechanisms are defined.

## **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.**

RMP information (OCA and non-OCA) can be accessed via Federal Reading Rooms – EPA and DOJ (Department of Justice) maintain Federal Reading Rooms (also known as Reading Rooms). Complete RMPs may be accessed via Reading Rooms which are open to the public, usually by appointment. Paper copies of up to 10 RMPs are provided for requesters. Requesters may read and take notes of the information contained in the RMP(s). However, the RMP(s) may not be removed, photocopied, or otherwise mechanically reproduced. Individuals who request to view RMPs must show photo identification issued by a federal, state, or local government agency such as a driver's license or passport. Requesters are required to sign a certification on a sign-in sheet, which is maintained by the Reading Room. Reading Room personnel keep records of Reading Room use and certifications in accordance with procedures established by the Administrator and the Attorney General. These records are retained for no more than three years. Reading Rooms do not index or otherwise manipulate the sign-in sheets according to individuals' names, except in accordance with the Privacy Act. For more information: Title 40, Part 1400, Subpart B – Public Access.



RMP information (non-OCA) can be accessed by submitting a Freedom of Information Act request via FOIAonline.

For federal, state, and local officials, who have a need to know can access RMP information (OCA and non-OCA) via their CDX RMP\*Info accounts.

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

The original purpose of the system was to collect specific information about RMP facilities for dissemination to the public in order for them to understand the risks in their immediate areas and to covered persons, states, and LEPCs for emergency response and preparation activities.

#### **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?**

The sharing of information by CDX and RMP is covered by a CDX MOU. If access to RMP information is needed by an external system in the future, a new MOU will be written.

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

Yes. See 4.1 for Federal Reading Rooms. To access RMP\*Info OCA and Download Dataset OCA, users must acknowledge a Security Notice which restricts how OCA data may be redistributed. Those restrictions do not apply to other sections.

#### **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:**

Risks evaluated:

- Laws and regulations are violated due to inappropriate collection of personal information.
- Laws and regulations are violated due to an organization failing to provide notices on usage of customer data.

##### **Mitigation:**

Any privacy risks identified in this system are mitigated by the security and privacy controls implemented in the SRMP SSP under 14.20 - AUTHORITY AND PURPOSE (AP). Mitigation considered:

- Legal authority is explicitly defined.
- Data classification (sensitive, non-sensitive, etc.) is conducted and the location or repositories of such is clearly defined.

## 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?

CDX roles and administrative settings are used to limit user access to only the functions and information for which they have been approved. Covered persons sign and/or acknowledge security notices indicating how information may be distributed. Facility Certifying Officials sign Electronic Signature Agreements regarding the information they submit and the use of their account. Once PII has been distributed to the public, there is no restriction on its use.

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

EPA staff who work with RMP data and the RMP Reporting Center staff read guidance documentation and take an associated test regarding the handling of Offsite Consequence Analysis (OCA) information included in the RMP. Due to the sensitivity of the OCA data, the entire database is handled in accordance with the guidance. The RMP Reporting Center staff distribute databases or provide the capability to access RMP information only as directed by EPA. Procedures for assigning system access to users are followed.

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

#### Privacy Risk:

Risks considered:

- Lack of a privacy program may result in the compromise of sensitive information due to loss of integrity or confidentiality.
- Laws and regulations are violated as a result of customers' data being modified.
- Customer information is improperly disclosed when transmitted to a third party.
- Critical business processes and sensitive data are compromised due to a flawed monitoring and inspection process.
- Employees, contractors or third-party users breach privacy because they are not aware or trained on information privacy requirements.
- Privacy laws and regulations cannot be enforced due to ill-defined policy.
- Laws and regulations are violated as a result of poor integration of privacy controls into system design and development.
- Laws and regulations are violated as a result of inaccurate accounting practices of disclosures of information.

There are no privacy impacts related to auditing and accountability.

#### Mitigation:

Any privacy risks identified in this system are mitigated by the security and privacy controls implemented in the SRMP SSP under 14.21 - ACCOUNTABILITY, AUDIT, AND RISK

MANAGEMENT (AR). Mitigation considered:

- A privacy officer is assigned and/or designated for the organization.
- Privacy impact assessment methodology and programs are defined for the organization.
- Service providers are subject to agency privacy requirements and held accountable for such.
- Privacy controls are subject to periodic review and inspection by a neutral internal department or other.
- Employees and other agency personnel received periodic privacy training.
- Reporting mechanism and responsibilities to regulatory bodies are defined.
- Privacy controls are made automated, where possible.
- Potential records are maintained, and a custodian of these records is identified.

## 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.

Data is electronically collected and stored in a database. Applications are available for users to query data or generate reports for analytical purposes. Some data is used for administrative purposes. The primary method for retrieving information is by facility name or ID.

### 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 primary method for retrieving information is by facility name or ID.

### 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?

SRMP does comply with the privacy controls dictated by EPA's General ISSP that was required for ATO. We have implemented all of the administrative, physical, and technical controls required by that document to safeguard the individual's information.

### 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:

Risks evaluated:

- Customer information is improperly disclosed.
  - Customer information is improperly disclosed when transmitted to a third party
- EPA regulations allow for the distribution of RMP data to the public via defined mechanisms.

Since the data is distributed to the public as required by law, there are no risks related to the use of the PII.

**Mitigation:**

Any privacy risks identified in this system are mitigated by the security and privacy controls implemented in the SRMP SSP under 14.27 - USE LIMITATION (UL). Mitigation considered:

- The usage of PII is limited to accepted personnel and tasks only.

**\*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:**