United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

Please submit your responses to your Liaison Privacy Official
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf.

If you need further assistance contact Marlyn Aguilar, at aguilar.marlyn@epa.gov or (202) 566-0012.

System Name: System for Risk Management Plans (SRMP)	
Preparer: M. Gérardin	**Office: OELM / OEM / RID**
Date: Submitted 31 August 2017 **Amended 8 November 2017**	**Phone: 202-564-2491**
Reason for Submittal: New PIA____ Revised PIA____ Annual Review____ Rescindment ____	
This system is in the following life cycle stage(s):	
Operation & Maintenance ☒	
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 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 (CSISSFRRA) 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 in an encrypted database that is inaccessable 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 agreements 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?

Yes. Both CDX and SRMP have System Security Plans.

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.

N/A

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

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 Uses of the Information

The following questions require a clear description of the system's use of information.

3.1 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.

3.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes-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 provide different types of information to users based on their level of access and the application used.

Types of Users and Information They Can Retrieve

- Covered Persons (as described on page 1 of this PIA), may query a downloaded MS Access database by any PII data element included in a Risk Management Plan. Personal identifiers include facility employees/representatives: Facility Owner/Operator Name, Facility Emergency Contact Name, RMP Preparer Name, and Name of Facility Representative Responsible for RMP Implementation.
- RMP Reporting Center Administrative Personnel may query the system by any of the data elements listed for Covered Persons (i.e., by any PII data element included in a Risk Management Plan). Personal identifiers include facility employees/representatives: Facility Owner/Operator Name, Facility Emergency Contact Name, RMP Preparer Name, and Name of Facility Representative Responsible for RMP Implementation, as well as by unique user identifiers assigned to individual users within RMP*Info and RMP*Download Dataset subsystems.

3.3 If the system retrieves information by personal identifier, what types/elements of information about the user are being retrieved?

Covered Persons:

- Once an RMP has been retrieved, users may view the facility address, title, and contact information (e.g. work phone number and work email address) for a Preparer, owner/operator, emergency contact, or Person Responsible for RMP Implementation (i.e., facility employees/representatives). They may also view the facility name, facility location address, and EPA Facility ID which would be work history linked PII.
- Reporting Center Administrative Personnel may view all of the information above, as well the internal unique identifiers for RMP*Info and RMP*Download Dataset users and the CDX User IDs associated with RMP Preparers and Certifying Officials.

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

None.

3.5 Does the system use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how EPA plans to use such results.

No.

3.6 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk:

None. 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.

Section 4.0 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.

4.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

CDX provides a Warning Notice and Privacy Statement to users during registration indicating the type of privacy information collected and its purpose. Users must agree to the terms and conditions before completing registration. The Warning Notice and Privacy Statement apply to subsystems hosted by CDX.

4.2 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?

Before potential CDX users can register for an account, they must acknowledge that they fully understand and consent to the 1) use policies (as listed in the Warning Notice) and 2) Privacy Statement. Both the Warning Notice and Privacy Statement appear on the CDX log-in page.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk:

None. Risks evaluated:

- Laws and regulations are violated due to an EPA failing to provide notices on usage of customer data.
- Laws and regulations are violated due to an organization failing to provide notices and privacy statements on usage of customer data.
- Absence of privacy communication and reporting processes leads to policy violations and security breaches.

Mitigation:

Any privacy risks identified in this system are mitigated by the security and privacy controls implemented in the SRMP SSP under 14.26 - TRANSPARENCY (TR). Mitigation considered:

- System banners (internal) and/or website notification (public) are in place to address the notification and usage of PII, where applicable.
- For applicable federal system, compliance with System of Records Notices criteria is followed.
  A privacy impact officer is identified for the organization (as applicable).

Section 5.0 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.

5.1 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.

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

No.

5.3 Who *(internal and external parties)* will have access to the data/information in the system? If contractors, are the Federal Acquisition Regulations (FAR) clauses included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act)?

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.

RMP data is also distributed to the public via Federal Reading Rooms, Local Emergency Planning Committees (LEPC), facilities, and FOIA requests.

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

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.

5.5 Explain how long and for what reason the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

EPA Records Schedule 0047.

5.6 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

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

5.7 Privacy Impact Analysis: Related to Retention

Privacy Risk:

None. 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 6.0 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.

6.1 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.

6.2 Describe how the external sharing noted in 6.1 is compatible with the original purposes of collection in the SORN noted in 3.4.

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. The sharing noted in 6.1 is consistent with the intended purposes outline in the in 6.1

6.3 Does the agreement place limitations on re-dissemination?

Yes. See 6.1 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.

6.4 Describe how the system maintains a record of any disclosures outside of the Agency.

See 6.1 for disclosures by DOJ-maintained Federal Reading Rooms. Access to RMP*Info OCA and Download Dataset OCA applications requires users to acknowledge a Security Notice. The acknowledgement of this Security Notice is

logged in the database. Distribution of data on DVD is also recorded in a log.

6.5 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.

6.6 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk:

None. 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 7.0 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.

7.1 What are the procedures that allow individuals to access their information?

Facilities submit RMPs to EPA and certify the RMP information is accurate and true to the best of their ability. Facilities are responsible for maintaining the information in their RMP, which includes facility employee/representative information (as listed above in *Section 2.1: Identify the information the system collects, uses, disseminates, or maintains*). They must resubmit their RMP at least once every five years or more often if certain changes have occurred. They are also required to correct their RMP within a certain time-frame if their emergency contact has changed or an accident has occurred. Users can correct certain registration information or contact CDX to have it changed. This is covered by CDX.

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

Facility Preparers can correct information about an individual listed in the facility RMP. CDX users contact CDX to update registration information.

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

CDX users are directed to first contact the CDX Help Desk for all questions and issues regarding their account. The CDX Help Desk can assist the user with the correction of registration information. Each facility is responsible for correcting information within its RMP.

7.4 Privacy Impact Analysis: Related to Redress

None. Risks evaluated:

- Laws and regulations are violated as a result of individuals not having the ability to access their personal information as stored by the agency.
- Laws and regulations are violated as a result of individuals not having the ability to choose how their personal information is to be used.
- Violations to privacy laws, and regulations cannot be enforced due to ill-defined policy.
- The extent of a security breach of personal information and possible damage(s) may not be identified.

Mitigation:

Any privacy risks identified in this system are mitigated by the security and privacy controls implemented in the SRMP SSP under 14.24 - INDIVIDUAL PARTICIPATION AND REDRESS (IP). Mitigation considered:

- Users sign-off on acceptable usage guidelines for PII.
- Users signoff on acceptable usage guidelines for PII, and have access to relevant information.
- Users may access applicable information through the concept of least privilege.
- An anonymous incident "hot-line" or similar should be available to employees for complaints, questions, and concerns.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the system ensure that the information is used in accordance with stated practices in this PIA?

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.

8.2 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.

8.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

None. 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.

Approval Signature

_____

Program Office, Liaison Privacy Official

_____

Marlyn Aguilar
Headquarters, Liaison Privacy Official

_____

Judy Earle
Agency Privacy Officer
Environmental Protection Agency

Original signed copy on file with the National Privacy Program.