



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: Office of Chemical Safety and Pollution Prevention Management Systems Salesforce (OIMSS)	System Owner: Jan Krysa
Preparer: William Northern	Office: OCSPP/OPS
Date: February 18, 2026	Phone: 202-566-1493
Reason for Submittal: New PIA ___ Revised PIA ___ Annual Review <u>X</u> Rescindment ___	
This system is in the following life cycle stage(s):	
Definition <input type="checkbox"/> Development/Acquisition <input checked="" type="checkbox"/> Implementation <input checked="" type="checkbox"/>	
Operation & Maintenance <input checked="" type="checkbox"/> Rescindment/Decommissioned <input type="checkbox"/>	
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>	
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>	

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

The OIMSS supports OCSPP Program Office's, the Office of Pesticide Programs (OPP), Office of Pollution Prevention and Toxics (OPPT) and the Office of Science Coordination and Policy (OSCP) by supporting development and hosting of applications for business processes, data collection, reporting, and workflow automation, supporting daily business operations at OCSPP. The OIMSS Salesforce Gov Cloud application resides in the General Support System boundary within the Office of Chemical Safety and Pollution Prevention Organization. The OIMSS will provide operations in the areas of program/project

monitoring and program evaluations for regulatory reviews, develop business workflow and business approval processes for streamlining work activities, and compute budget allocations based on program/project requests. It allows multiple groups to view information available in real time settings and synthesizes data by producing statistical reports.

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?

Atomic Energy Act, 42 U.S.C. §2011 et seq. (1954)

Clean Air Act, 42 U.S.C. §7401 et seq. (1990)

Design for the Environment, 7 U.S.C. §136w-8 (2012)

Emergency Planning and Community Right-to-Know (EPCRA), 42 U.S.C. §11001 et seq. (1986)

Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA), 7 U.S.C. §136 et seq. (1996)

Federal Information Technology Acquisition Reform Act (FITARA), 40 U.S.C. 101 §3601 (2002)

Frank R. Lautenberg Chemical Safety for the 21st Century Act, 15 U.S.C. 2601 (2016)

Information Collection and Paperwork Reduction Act (PRA), [44 U.S.C. § 101](#); [44 U.S.C. § 3501](#) et seq (1986)

Pollution Prevention Act (PPA) 44 USC §3501 et seq. (1990)

Toxic Substance Control Act (TSCA), 15 U.S.C. §2601 et seq. (1976)

Waste Isolation Pilot Plant Land Withdrawal Act, U.S.C. 1996 LWA Public Law 102-579

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 SSP has been completed for the system. The ATO expired May 31, 2026.

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 2070-0075; Title: TSCA CBI Access Request, Agreement, and Approval

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?

Data will be stored in the Cloud. Cloud Service Provider is FedRamp approved. The service type is 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).

Information collected:

- Name
- Address Name– work
- Program organization
- Telephone number-office, cell
- Email address
- Financial information collected on: Contracts, Grants, IAs, Training and Travel
- Document Control Number (DCN) associated with each project
- Chemical Pesticide Data
- Chemical Incident Response (name of person reporting incident, location of incident, type of incident)

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

Data is collected from internal and external sources. Internal sources are by EPA users (contractor and employees) who input data into the various systems, creating statistical reports. Data is imported from EPA's Finance Central and Pesticide Registration Information System (PRISM) that is used for data integration from different platforms. External users, i.e. public users, industry and community organizations input data in the various systems available in the Salesforce organizational chart.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Yes, commercial/industry, public users do submit data for the OCSPP to use for daily business operations. Information is collected to conduct analysis, assessments, evaluations and regulatory decisions. The information is used to manage chemical review processes and risk assessments, generate statistical data for Information Collection Requests (ICRs), manage organizational records to promote the use of energy efficient technologies, maintain industry contract records, communicate status reports on policy initiatives and decisions, and generate stake-holders status reports. These reports are also stored in OIMSS but not retrievable by PII.

2.4 Discuss how accuracy of the data is ensured.

The systems require user authentication and uses data validation tools to determine data accuracy. Some systems require levels of approval to ensure data accuracy.

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:

The risk comes from unauthorized access to this PII. An unauthorized individual can gain access to this in one of two ways: they actively are able to access the system; or someone who is authorized provides the information to them.

Mitigation:

Information will be maintained in a FedRamp-approved platform with a moderate ATO and annual security assessments will be conducted. Access controls are in place to ensure only those authorized and have a need-to-know may access the data. EPA users are provided annual Information Security Privacy Awareness Training (ISPAT) and sign Rules of Behavior (RoB).

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?

The system has permission rights and designated roles for authorized users. General users have access to information on a need-to-know basis. Administrative users have elevated rights to manage the system and user accounts.

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

System user access is approved based on the job duties. The user access request profile is completed and submitted to the supervisor for approval. The System Technical Lead processes the user access request for final approval status. User account access control procedures are established using the Salesforce User Manual, User Management Administration section.

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

Yes

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 who provide operational and maintenance support to the system. The appropriate FAR clauses are included in the contract that grants contractor access to the system data/information.

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.

How long and for what reasons information is retained varies depending on the data type. OIMSS uses several retention schedules listed below that dictate how and when information should be destroyed or archived.

EPA Records Schedule 0054

- Item a:** (Reserved)
- Item b:** (Reserved)
- Item c:** Electronic data

CUI//ISVI

This item is to be used only by the Office of the Chief Financial Officer, Office of Technology Solutions at Headquarters.

- NARA Disposal Authority: N1-412-94-2/6c
- **Disposable**
- Maintain individual records 6 years and 3 months after final payment, then delete when no longer needed unless related to the Superfund program cost recovery efforts (see Agency-wide Guidance).

Item d: (Reserved)

Item e: (Reserved)

EPA Records Schedule 0329

Item a: Electronic software program

The Office of Chemical Safety and Pollution Prevention, Office of Pesticide Programs, Information Technology and Resources Management Division, Information Services Branch at Headquarters is responsible for the disposition of this item.

- NARA Disposal Authority: N1-412-09-16a
- **Disposable**
- Destroy when no longer needed to ensure access to, and use of, the electronic records throughout the authorized retention period.

Item b: Input

- NARA Disposal Authority: DAA-0412-2013-0009
- **Disposable**
- Follow instructions for schedule 1012.

Item c: Registration and registration review data and documents

Includes end use product data, labeling and PRIA data.

- NARA Disposal Authority: N1-412-09-16c
- **Permanent**
- Close inactive records at completion of action.
- Transfer data to the National Archives annually after file closure and completion of any ongoing audits involving review of data and documents, with any related documentation and external finding aids, as specified in 36 CFR 1235.44-1235.50 or standards applicable at the time.

Item d: (Reserved)

Item e: (Reserved)

Item f: Reference and information tracking databases

- NARA Disposal Authority: N1-412-09-16f
- **Disposable**
- Follow instructions for applicable schedule (EPA 0088, EPA 0089).

Item g: Output and reports

- NARA Disposal Authority: Varies
- **Varies**

CUI//ISVI

- File with related records and follow instructions for the related records.

Item h: System documentation

The Office of Chemical Safety and Pollution Prevention, Office of Pesticide Programs, Information Technology and Resources Management Division, Information Services Branch at Headquarters is responsible for the disposition of this item.

- NARA Disposal Authority: N1-412-09-16h
- **Permanent**
- Transfer to the National Archives those records necessary to document how the system captures, manipulates and outputs data, as specified in 36 CFR 1235.44-1235.50 or standards applicable at the time. The documentation is transferred with the electronic data, item c.

EPA Records Schedule 1005

Item a: Budget records

Includes, but is not limited to:

- Apportionment and reapportionment schedules, proposing quarterly obligations under each authorized appropriation.
- Background records, cost statements, rough data and similar working papers accumulated in the preparation of annual budget estimates, including duplicates of budget estimates and justifications and related apportionment language sheets, narrative statements, copies of transcripts of congressional budget hearings, and related documents; and
- Reports generated and received throughout the budget process, including copies of the annual budget, as well as periodic reports on the status of appropriation accounts and apportionment and documents authorizing new or revised budget allowances to programs (excludes the record copy of the annual budget submitted to the Administrator, the Office of Management and Budget (OMB), and the President which is permanent and covered by schedule 299, item c(1)).

- NARA Disposal Authority: DAA-0412-2013-0020-0001

- **Disposable**

- Close at end of fiscal year covered by the budget or when no longer needed for current agency business.
- Destroy 5 years after file closure.

Item b: Financial transaction records

Includes, but is not limited to, records related to procuring goods and services, paying bills, collecting debts, and accounting:

- Accountable officers' files maintained by the Agency for site audit by the Government Accountability Office (GAO) auditors, consisting of statements of transactions, statements of accountability, collection schedules and

CUI//ISVI

vouchers, disbursement schedules and vouchers, and all other schedules and vouchers, or documents used as schedules or vouchers (excludes commercial freight charges for services for fiscal accounts that are not settled and payroll records covered by other items in this schedule);

- Appropriation allotment files, showing status of obligations and allotments under each authorized appropriation;
- External accounting reports as required by government-wide regulations; and
- General accounting ledgers, showing debit and credit entries, and reflecting expenditures in summary.
- NARA Disposal Authority: DAA-0412-2013-0020-0002
- **Disposable**
- Close after final payment or cancellation, or when end of fiscal year has occurred, or when fiscal year close-out activities are concluded, or when period covered by the account has ended.
- Destroy 6 years after file closure.

Item c: Payroll support

Includes: employee status reports for employee's statement data, prepared biweekly, quarterly, and annually.

- NARA Disposal Authority: DAA-0412-2013-0020-0003
- **Disposable**
- Close at end of pay cycle.
- Destroy 56 years after file closure.

Item d: Payroll records not covered elsewhere

Includes, but is not limited to:

- Combined Federal Campaign and other allotment authorizations, such as union dues and savings;
- Leave application files, if employee has not electronically submitted their time card or equivalent;
- Payroll control consisting of worksheets, reconciliation reports, redistribution of disbursement between appropriations, and related records; and
- Payroll system reports, including error reports, ticklers, system operation reports, reports and data used for workload and/or personnel management purposes.
- NARA Disposal Authority: DAA-0412-2013-0020-0004
- **Disposable**
- Close after GAO audit or when 3 years old, whichever is sooner.
- Destroy immediately after file closure.

Item e: Individual employee pay record

Includes: individual employee pay folders consisting of payroll allotments, state tax forms, and related records.

- NARA Disposal Authority: General Records Schedule 2/1b
- **Disposable**
- Close after employee leaves the Agency.
- Transfer to the National Personnel Records Center. Destroy 56 years after file closure.

Item f: Time and attendance source records

CUI//ISVI

Includes: source records consisting of forms for payroll processing.

- NARA Disposal Authority: General Records Schedule 2/7
- **Disposable**
- Close after GAO audit or when 6 years old, whichever is sooner.
- Destroy after file closure.

Item g: (Reserved)

Item h: (Reserved)

EPA Records Schedule 0758

Item a: Electronic data, except import and export records covered by item b
This item is to be used only by the Office of Chemical Safety and Pollution Prevention (OCSPP), Office of Pollution Prevention and Toxics (OPPT) at Headquarters.

NARA Disposal Authority: DAA-0412-2015-0004-0001

- **Permanent**
- Close when program is discontinued, or system is terminated.
- While system is in operation, transfer a copy of the data as specified in 36 CFR 1235.44-1235.50 or standards applicable at the time, to the National Archives every 5 years. Transfer final data to the National Archives 6 months after system is closed.

Item b: Electronic data - import and export records for TSCA Section 12(b) and Section 13 submissions

This item is to be used only by the Office of Chemical Safety and Pollution Prevention (OCSPP), Office of Pollution Prevention and Toxics (OPPT) at Headquarters.

NARA Disposal Authority: DAA-0412-2015-0004-0001

- **Disposable**
- Close when activity, project, or topic completed.
- Destroy 5 years after file closure.

EPA Records Schedule 1035

Item a: Historically significant environmental program and project records
Includes substantive program and project records within one or more of the following categories: that assess ongoing threats to human health and the environment; that document significant actions to improve air quality, reduce risks associated with exposure to toxic substances, or protect water from contaminants

CUI//ISVI

that endanger public health; that produce major contributions to environmental or scientific knowledge; that result in new and advanced technologies and methodologies; and that have continuing research and informational value beyond EPA's use of the records for business purposes.

- NARA Disposal Authority: DAA-0412-2013-0021-0001
- **Permanent**
- Close when activity, project, or topic completed.
- Transfer to the National Archives 15 years after file closure.

Item b: Long-term environmental program and project records

Includes records that are not required for documenting the history of the program or project, but which have operational value to EPA throughout the life of the program or project.

- NARA Disposal Authority: DAA-0412-2013-0021-0002
- **Disposable**
- Close when activity, project, or topic completed.
- Destroy 20 years after file closure.

Item c: Routine environmental program and project records

Includes records with routine operational value and not considered essential for the ongoing management of the program or project.

- NARA Disposal Authority: DAA-0412-2013-0021-0003
- **Disposable**
- Close when activity, project, or topic completed.
- Destroy 10 years after file closure.

Item d: Short-term environmental program and project records

Includes records with short-term operational value and not considered essential for the ongoing management of the program or project.

- NARA Disposal Authority: DAA-0412-2013-0021-0004
- **Disposable**
- Close when activity, project, or topic completed.
- Destroy 5 years after file closure.

Item e: Other environmental program and project records

CUI//ISVI

Includes records that have no value once they are superseded, updated, replaced, or no longer needed for the ongoing management of the program or project.

- NARA Disposal Authority: DAA-0412-2013-0021-0005
- **Disposable**
- Close when superseded, updated, replaced, or no longer needed for current agency business.
- Destroy immediately after file closure.

EPA Records Schedule 0352

Item a: (Reserved)

Item b: Electronic data for Incident Data System (IDS)

The Office of Chemical Safety and Pollution Prevention, Office of Pesticide Programs, Information Technology and Resources Management Division, Information Services Branch at Headquarters is responsible for the disposition of this item.

NARA Disposal Authority: N1-412-05-7b

- **Permanent**
- Transfer to the National Archives when 50 years old, as specified in 36 CFR 1235.44-1235.50 or standards applicable at the time.

Item c: Source documents (reports)

NARA Disposal Authority: N1-412-05-7c

- **Disposable**
- Close file annually.
- Destroy 20 years after file closure.

Item d: (Reserved)

Item e: (Reserved)

Item f: (Reserved)

EPA Records Schedule 0089

Item a: Record copy

Includes tracking and control records used to provide access to and control of records authorized for destruction by the GRS or a NARA-approved records schedule, including indexes, lists, registers, inventories, and logs.

Excludes records containing abstracts of records content or other information that can be used as an information source apart from the related records which are covered by the schedules for the content (e.g., enforcement, permits).

NARA Disposal Authority: DAA-GRS-2013-0002-0016

- **Disposable**
- Close when no longer needed for current agency business.

- Destroy immediately after file closure.

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:

Contact information is maintained primarily as part of the official record, according to EPA schedules regardless of the continued existence of an organizations change in ownership. The risks are the data is kept for too long of a time period.

Mitigation:

Archive or destroy outdated business records to decrease OIMSS exposure to identity theft and business fraud.

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.

OCSPP and OAR do share information to external resources in conjunction with normal agency operations to organizations and stakeholders. The information is shared through various general communications (email, press release, phone calls), newsletters, program websites, policy and regulation reports, not through MOUs or MOAs. Often times these communications are a collection of non-PII data submitted by external organizations and stakeholders. The external organizations and stakeholders do not have direct access into OIMSS.

Second, EPA follows standard Information Collection Review (ICR), namely the Federal Register public comment periods to allows external users to submit comment in response to new and revised regulatory requirements.

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

The external sharing allows industry, organizations and community stakeholders to submit information and comments that can be used in the program assessment and evaluations for

chemical policies and regulatory actions.

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 Technical Lead and System Administrators are the responsible parties that approve information sharing agreements and user accounts.

4.4 Does the agreement place limitations on re-dissemination?

The system requires users to understand and agree to abide by the ROB after the user account has been established and after system updates. The ROB addresses information sharing and re-dissemination of information with the proper approvals/clearances.

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:

The system only shares information on regulatory decisions and what's publicly available on the system websites. The risk is related to human error.

Mitigation:

The information is protected by access controls which limit its confidentiality and availability to the authorized users. EPA personnel are required to take Annual Security and Privacy Awareness Training. Should human error be the cause of the unauthorized information sharing, the individual will need to take additional training.

[OBJ:OBJ] 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?

Users are entrusted to adhere to the ROB regarding the use, dissemination and protection of the information in their possession. Additionally, the system provides audit records for: System alerts and error messages; User/Admins logon and logoff; System administration activities; Account creation, modification, or deactivation; Modifications of privileges and

CUI//ISVI

access controls; Additional security-related events, as required by the information or system owner; Application/System alerts and error messages, and configuration changes.

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

Internal system users must complete an annual information security and privacy awareness training that addresses the use and handling of privacy information. External users are entrusted to adhere to the ROB as part of their limited user access privileges.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Unauthorized access jeopardizes accountability and puts the following privacy related information at risk: Names, business emails, business phone numbers, and business addresses for borrowers. If the system is unable to associate access to the system with an authorized individual, then this poses a great risk to accountability. Further risk is incurred when the auditing functions of the system do not properly capture access to the system; i.e. successful and failed login attempts.

Mitigation:

To mitigate risk, the OPS Salesforce Team authorizes requests for access from users. Account access is setup to limit borrowers to their organization's data. Auditing capabilities are in place in the GSS (OIMSS) hosting environment. The OIMSS SSP (AU-2) reads in part, "The OIMSS application is currently configured to capture activity performed by any user within the application, when the action was attempted, the details of the event, and the identity of any individuals or subjects associated with the event. This allows for thorough security audit reviews as well as troubleshooting of any potential issues within the application.

In real-time, the system provides audit records for: System alerts and error messages; User/Admins logon and logoff; System administration activities; Account creation, modification, or deactivation; Modifications of privileges and access controls; Additional security-related events, as required by the information or system owner; Application/System alerts and error messages, and configuration changes."

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.

Information is collected to conduct analysis, assessments, evaluations and regulatory decisions. The information is used to manage chemical review processes and risk assessments, generate statistical data for ICRs, manage organizational records to promote the use of energy efficient technologies, maintain industry contract records, communicate status reports on policy initiatives and decisions, and generates stake-holders status reports.

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.)*

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 OIMSS Salesforce Gov Cloud application resides in the General Support System boundary within the Office of Chemical Safety and Pollution Prevention Organization. This GSS has an ATO compliant with SP 800-53 security controls and EPA security standards. The application itself has access controls in the form of required logon and prior authorization is required to obtain an account.

GSS follows EPA CIO directives, policies, and procedures. OIMSS is not set up to search for information using an individual's PII.

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:

Information may only be used for the intended purpose previously described in the "general description/overview" section of this document (page 1). The risk to "uses of information" occurs when information is used for unintended purposes. For example, not related to management of loan closures. This jeopardizes the EPA's trust with the public and could discourage future borrowers.

Mitigation:

EPA users read and sign Rules of Behavior annually. The OIMSS SSP (AU-2) reads in part, “The OIMSS application is currently configured to capture activity performed by any user within the application, when the action was attempted, the details of the event, and the identity of any individuals or subjects associated with the event. This allows for thorough security audit reviews as well as troubleshooting of any potential issues within the application.

***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 use, 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:

I attest as the Agency Privacy Officer that **Office of Chemical Safety and Pollution Prevention Management System Salesforce (OIMSS)** Privacy Impact Assessment (PIA) has been reviewed. The privacy implications have been adequately identified with appropriate mitigation statements included for implementation in the development or use of information technology systems.

Respectfully,

Lee Kelly
Agency Privacy Officer
Cybersecurity Planning & Risk Mgmt Branch
EPA/OFA