United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 07/2018)

Please submit your responses to your Liaison Privacy Official
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf. If you need further assistance, contact your LPO.

System Name: Office of Chemical Safety and Pollution Prevention Management Systems Salesforce (OIMSS)	
Preparer: Tony Cheatham	**Office: OCSPP/OPPT**
Date: 03/18/2020	**Phone: 202-564-8594**
Reason for Submittal: New PIA__X__ Revised PIA____ Annual Review____ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☒	
Operation & Maintenance ☐ Rescindment/Decommissioned ☐	

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 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. 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.

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?

SSP has been completed for the system. The system has an ATO the expire in 07/18/2020 but will be issued a new ATO due a major change in environment after the Security Assessment is completed and Findings and Recommendations remediated.

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 – 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

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 users who input data into the various systems. Data is imported from Finance Central and 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.

Information is provided by commercial/industry submitters and public users. 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.

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:

None. The data is collected from external users after a user account profile has been established.

User ID and password is provided to access the system and data is populated in the system.

Mitigation:

None.

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

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.

The information is based on the EPA Records Control Schedule for the designated program office.

No.	Title	Function	Program	Applicability	Revised
0054	Compass Financials (Compass) OIMSS tracks program budget allocations and supporting data exported from Compass.	402	Financial Management	Headquarters	04/30/2014
0329	Pesticide Registration Information System (PRISM) Registration information is imported/exported for program regulatory reviews, evaluations and decisions.	108	Pesticides	Headquarters	12/31/2013
1005	Financial Management OIMSS tracks program budget allocations and supporting data exported from EAS.	402	Financial Management	Agency-wide	04/30/2017

0758	Chemical Information System (CIS) TSCA chemical information is imported/exported for program regulatory reviews, evaluations and decisions.	108	Toxic Substances	Headquarters	04/30/2016

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:

There is no risk to this information being retained for extended amounts of time. Contact information is maintained primarily as part of the official record, according to EPA schedules regardless of the continued existence of a company or change in ownership.

Mitigation:

None

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.

ICR information is shared through OMB that allows external users to submit comment in response new and revised regulatory requirements.

OCSPP and OAR does share information to external resources in conjunction with normal agency operations to organizations and stakeholders. The information is shared through various communications (email, press release, phone calls), newsletters, program websites, policy and regulation reports.

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 Administers 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 agree to the ROB after the user account has been established and after system updates. The ROB addresses information sharing and re-dissemination of information.

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

None, the system only shares information on regulatory decisions and what's publicly available on the system websites.

Mitigation:

None.

Section 5.0 Auditing and Accountability

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

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

Users are entrusted to adhere to the ROB regarding the use, dissemination and protection of the information in their possession.

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

Internal system users have to 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 user access privileges.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:
No privacy information is shared by internal or external users.
Information shared is publicly available on the system websites and from other stakeholders resources.

Mitigation:
Internal users compete Agency annual security awareness training that addresses information sharing and the handling of privacy data.

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.*)

Project Number or Workflow Number.

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

None

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 according to the specific data collection guidelines.

Mitigation:

All internal and external uses adhere to the system ROB.

*If no SORN is required, STOP HERE.

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

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

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

Mitigation:

Section 8.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

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

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

8.4 Privacy Impact Analysis: Related to Redress

Privacy Risk:

Mitigation: