United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official.
All entries must be Times New Roman, 12pt, and start on the next line.
If you need further assistance, contact your LPO. A listing of the LPOs can be found here:
https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

System Name: OCSPP Cloud System	**System Owner: Leo Gueriguian**
Preparer: William Northern	**Office: OCSPP/OPS/ITRMD/IMTB**
Date: 04/03/2025	**Phone: 202-566-1493**
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:

OCSPP Cloud System will support Office of Chemical Safety and Pollution Prevention Organization (OCSPP) Program Offices, to include the Office of Pesticide Programs (OPP), Office of Pollution Prevention and Toxics (OPPT) and the Office of Program Support (OPS) in the development and hosting of applications for business processes, data collection, reporting, and workflow automation. This support is essential for the daily operations of OCSPP. The OCSPP Cloud System will provide operations in the areas of program/project monitoring and program evaluations for regulatory reviews, develop business workflows and business approval processes for streamlining work activities, and computing budget allocations based on program/project requests. The OCSPP Cloud System Gov Cloud application resides in the General Support System boundary within the OCSPP.

The system will allow multiple groups to access and view information in real-time and will synthesize 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?

No, the system is in the planning phase. OCSPP Cloud System security plan and supporting documentation is being created and will be finalized prior to implementation.

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: Please refer to page 16 Section 8.4 APPENDIX A: OCSPP Forms covered by the Paperwork Reduction Act (PRA)

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, data will be maintained in the Cloud. The Cloud Service Provider, Amazon Web Services is Fedramp approved. The OCSPP Cloud System will utilize PaaS and IaaS from the CSP.

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).

OCSPP CLOUD SYSTEM integrates information from OCSPP CLOUD SYSTEM source applications. PII information that is integrated and stored with OCSPP CLOUD SYSTEM relates to contact information for individuals who have been identified by a regulated facility as a contact for a regulated facility. The data elements stored by OCSPP CLOUD SYSTEM, when provided by OCSPP CLOUD SYSTEM source systems, are:

- EPA staff name, work address, work email address, work phone number, workforce ID, LAN ID, FIFRA CBI clearance status, EPA Office numbers
- EPA Office Numbers
- Federal and State enforcement personnel names
- Submitter's name and organizational contact information (company name, company address, company phone, email address, etc.).
- Study author name(s).
- Registrants contact name, email address, phone number
- Documents carried through the e-submission application may contain names, email addresses, phone numbers
- Type of incident(s)
- Product information
- Aggregate and individual incident reports
- Company contacts name, business phone number, business email
- Contractor information
- Contract / work order numbers
- Individual PII
    - Full name
    - Email address
    - Date of Birth
    - Phone number
    - Geographical data (city, state, zip code)
    - Employment information (job title, company name)
    - Public social media handles

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 (employees and contractors) who input data into the various systems, creating statistical reports. Data is imported from Salesforce; EPA's Active Directory system (AD) (EPA Staff) and EPA's Central Data Exchange (CDX) (Business Community) data is pushed to OCSPP Cloud System 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 AWS 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 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 the 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 generates stake-holders status reports. These reports are also stored in OCSPP CLOUD SYSTEM but not retrievable by personal identifier or other symbol assigned to an individual.

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. Quality Assurance is maintained via SOPs, data curation, and crowd sourcing. Audit and archival data are maintained at the row level.

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:

There is a risk of compromise of PII processed, including on hosted systems by an unauthorized individual.

Mitigation:

We deploy NIST 800-53 privacy and security controls to secure the system and information likely to be processed. Information will be maintained in a FedRAMP-approved platform with a moderate ATO. Controls include annual security assessments and access controls that ensure only those authorized and have a need-to-know have 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?

Access controls implemented on the system are specified in EPA's Access Control Policy located here.

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

Yes. Various application-specific security roles such as superuser and user exist with a more refined authorization within applications can be set for each role to allow the user access based on a need-to-know basis.

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?

Only EPA federal and contractor personnel with EPA network credentials, obtained through the Agency's standard process of network credential control and management have access to the OCSPP CLOUD SYSTEM. The OCSPP CLOUD SYSTEM is a platform, such as SharePoint or the National Computer Center. Applications, each owned and managed by Application Owner, run on it. If an Application Owner grants access to the Application Owner's application to a contractor and FAR clauses need to be in their contract, the Application Owner is responsible for ensuring compliance. The platform administrator does not have insight into the status of FAR clause inclusion in the contracts of contractors among the application's user base.

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. OCSPP Cloud System uses several retention schedules listed below that dictate how and when information should be destroyed or archived. For a list of the nine data types stored in OCSPP Cloud System refer to section 2.1. OCSPP CLOUD SYSTEM is not used to retrieve PII.

EPA Records Schedule 0054

Electronic data--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
- 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).

EPA Records Schedule 0329

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
- Destroy when no longer needed to ensure access to, and use of, the electronic records throughout the authorized retention period.

Input

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

Registration and registration review data and documents. Includes end use product data, labelling and PRIA data.

- NARA Disposal Authority: N1-412-09-16c
- 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.

Reference and information tracking databases

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

Output and reports

- NARA Disposal Authority: Varies
- File with related records and follow instructions for the related records.

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
- 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

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
- 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.

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 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
- 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.

EPA Records Schedule 0758

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

- 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.

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

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

EPA Records Schedule 1035

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 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
- Close when activity, project, or topic completed.
- Transfer to the National Archives 15 years after file closure.

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
- Close when activity, project, or topic completed.
- Destroy 20 years after file closure.

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
- Close when activity, project, or topic completed.
- Destroy 10 years after file closure.

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

Other environmental program and project records
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
- Close when superseded, updated, replaced, or no longer needed for current agency business.
- Destroy immediately after file closure.

EPA Records Schedule 0352

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

Source documents (reports)

- NARA Disposal Authority: N1-412-05-7c
- Close file annually.
- Destroy 20 years after file closure.

EPA Records Schedule 0089

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

- 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:

There is a risk that information might be retained longer than authorized.

Mitigation:

We review record retention schedules to ensure information is retained longer than authorized. OCSPP CLOUD SYSTEM administrators will either archive or destroy outdated business records following EPA retention schedules described in section 3.5 to decrease 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.

Yes. OCSPP CLOUD SYSTEM data is shared with the FedRAMP approved system called AWS Enterprise Cloud outside the Agency. The Agency has contractual agreements with AWS.

Some information in OCSPP CLOUD SYSTEM is shared outside 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 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 OCSPP CLOUD SYSTEM. Information available on the public search pages is considered public information and is non-confidential.

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

External sharing allows industry, organizations and community stakeholders to submit information and comments that can be used in EPAs program assessment and evaluations for chemical policies and regulatory actions to ensure accuracy of EPA's work. FIFRA security requirements include very limited external access under limited conditions. Administrator-level approval is required under those circumstances. FIFRA security procedures are managed by authorized officials to ensure alignment with the existing purposes as detailed in FIFRA.

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?

Contract arrangement with AWS, Interconnection Security Agreements (ISAs), and Memorandum of Understandings (MOUs) are used as needed for other systems with dedicated interconnections. As stated in supplementary guidance in CA-3 Interconnection agreement, interconnection security agreements would be set up for "dedicated inter-connections".

4.4 Does the agreement place limitations on re-dissemination?

AWS has a contractual agreement and provides data on a need-to-know basis as defined between roles and refined permission sets.

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 privacy risk is related to human error where an employee may share information to unintended individuals.

Mitigation:

The information is protected by access controls which limit its availability to 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.

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?

The Office of Program Support monitors the design, maintenance, administration, and use of OCSPP CLOUD SYSTEM for adherence to security and privacy standards. OPS holds a Conceptual Review of each OCSPP CLOUD SYSTEM application as it is being architected and designed. OPS reviews the applications data entities, relationships, user community, including roles and responsibilities and license requirements, etc. The use of shared objects and any restrictions on use of data is reviewed as well. The System owner must commit to adherence to any such restrictions and to passing those restrictions to the application and its users. OPS holds an Architectural Review of the application once it has been designed in detail, to assure that OCSPP CLOUD SYSTEM's structure and data is in accordance with the approved conceptual design, including any restrictions on data use. Finally, OPS holds a Production Readiness Review to assure that the application has been tested and found in compliance with the approved design and all applicable data restrictions. 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 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.

This is a function of the Agency source systems that collect the data. This is an agency requirement to ensure all employees take the annual Security and Privacy Awareness Training.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

There is a risk that auditing functions of the system do not properly log access to the system, i.e. successful and failed login attempts. 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.

Mitigation:

Auditing capabilities are in place in the OCSPP Cloud System environment. The OCSPP CLOUD SYSTEM SSP (AU-2) reads in part, "The OCSPP CLOUD SYSTEM 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."

Privacy risk attaching to the operation of this system is reviewed periodically and the system is also continuously monitored.

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. He 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.)

The primary organization of the OCSPP CLOUD SYSTEM is not by person, but by application.

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 OCSPP Cloud System holds an Architectural Review of the application once it has been designed in detail, to assure that the application's structure and data is in accordance with the approved conceptual design, including any restrictions on data use.

This PIA process is the primary procedure for assessing privacy risk, and it is done periodically and as needed.

Additionally, each source system that processes PII could have its own SORN, but as a secondary user of the information, no SORN is known to apply to the Platform. In cases where OCSPP Cloud System stores and transmits sensitive data collected by a source system, the source system would be responsible for the SORN.

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:

There is a risk that information could be used for other than authorized purposes and/or by unauthorized persons.

Mitigation:

Access controls on Cloud System and hosted applications ensures only those with need to know have access to systems and data. OCSPP Cloud System requires multifactor login using Agency LAN ID and password in accordance with FISMA Moderate level controls specified in the OCSPP Cloud System security plan. Dissemination of sensitive information is further restricted based on

authorization to those users specifically with a need-to-know. Periodic reviews ensure data is used for authorized purposes and persons 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:

8.4 APPENDIX A: OCSPP Forms covered by the Paperwork Reduction Act (PRA)

- OMB Control number 2070-0075; Title: TSCA CBI Access Request, Agreement, and Approval.
- OMB Control number 2070-0020; Title: FIFRA Access Authorization Agreement.
- OMB Control number 2070-0060: Title: Application for Pesticide Registration / Amendment - EPA Form 8570-1 (pdf)
- OMB control number ## Title: Confidential Statement of Formula - EPA Form 8570-4 (pdf)
- OMB control number 2070-0044 Title: Notice of Supplemental Distribution of a Registered Pesticide Product - EPA Form 8570-5 (pdf)
- OMB control number 2070-0040 Title: Application for an Experimental Use Permit - EPA Form 8570-17 (pdf)
- OMB control number 2070-0182 Title: Application for/Notification of State Registration of a Pesticide To Meet a Special Local Need - EPA Form 8570-25 (pdf)
- OMB control number 2070-0060, 2070-0057, 2070-0107, 2070-0122, 2070-0164. Title: Formulator's Exemption Statement - EPA Form 8570-27 (pdf)
- OMB control number 2070-0182 Title: Certification of Compliance with Data Gap Procedures - EPA Form 8570-28 (pdf)
- OMB control number 2070-0057; 2070-0107; 2070-0122; 2070-0164 Title: Certification of Attempt to Enter into an Agreement with Registrants for Development of Data - EPA Form 8570-32 (pdf)
- OMB control number 2070-0226 Title: Certification with Respect to Citations of Data - EPA Form 8570-34 (pdf)
- OMB control number 2070-0226 Title: Data Matrix - EPA Form 8570-35 (pdf)
- OMB control number 2070-0060 Title: Summary of the Physical/Chemical Properties - EPA Form 8570-36 (pdf)
- OMB control number 2070-0060; 2070-0057; 2070-0107 Title: Self-Certification Statement for the Physical/Chemical Properties - EPA Form 8570-37 (pdf)
- Summary of the Physical/Chemical Properties and Self-Certification Statement for the Physical/Chemical Properties - Pesticide Registration Notice PR 98-1 (pdf)