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: Pesticide Environmental Stewardship Program Membership Platform (Salesforce)	**System Owner: Delores Barber**
Preparer: Frank Ellis	**Office: OCSPP/OPP**
Date: 05/10/2021	**Phone: 703-308-8107**
Reason for Submittal: New PIA____ Revised PIA____ Annual Review__X__ 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:

Salesforce is cloud-based Customer Relationship Management platform that supports the Pesticide Environmental Stewardship Program (PESP) and is managed by the Office of Pesticide Programs. It is used to market EPA's voluntary partnership program to the nation's pesticide user community, collect pesticide use and training data on member's Integrated Pest Management measures to reduce human health and environmental risks associated with pests and pesticides and to assess their progress and retention.

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?

- Sections 2(b), 3(b) and 4(b) of the Pollution Prevention Act of 1990, 42 U.S.C. 13 l0l(b)
- Section 3 of the Federal Insecticide, Fungicide and Rodenticide Act (FIFRA)
- Food Quality Protection Act of 1996 (7 USC 136r-l)

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 04/21/2023.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

- 0MB Control No: 2070-0188
- PESP Membership Application Form - EPA Form 9600-02
- PESP Strategy/ Progress Reporting Form for Residential/ Commercial Pest Control
- Providers Members - EPA Form 9600-03
- PESP Strategy/ Progress Reporting Form for All Members that are Not Residential /
- Commercial Pest Control Services Providers - EPA Form 9600-01
- The forms are available here: https://www.reginfo.gov/public/do/PRA ViewDocument?ref nbr=2016 I l-2070-002

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?

The data will be maintained in a Cloud on the Salesforce platform.
Salesforce is FedRAMP approved.
The service provider is a Paas and SaaS

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).

The system collects and maintains the company name, mailing address, industry type, business telephone number, name and title of primary and secondary company contact person, email address and telephone number of primary and secondary contact person, Organizational Profile Measures and 1PM Implementation and Adoption Progress Data (TPM Practices, pesticide risk reduction and usage, economic benefits, and IPM/Education and Promotion). The information collected by the system is restricted to the company/organizational level. No PII is used as an identifier.

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

Prospective applicants and PESP members submit electronic forms (PESP Membership Application and/or Strategy/Reporting forms) expressing a desire to join the program and to document their 1PM progress and commitment. EPA staff would enter the company's submitted information (assessments, correspondences, and other documentation) into Salesforce.

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. Information is voluntarily submitted electronically by PESP member representatives to the PESP Salesforce account via OPP's Data Exchange.

2.4 Discuss how accuracy of the data is ensured.

Participating PESP members are audited by an approved, third party certifying company.

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 ISAT and sign 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?

Role-based access is defined for each user (currently 3 users). The site administrator is responsible for assigning users to the appropriate role.

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

The Standard Operating Procedure for the PESP Salesforce system contains this policy/procedure.

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

No.

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

Only EPA (OPP/BPPD) staff that are FIFRA CBI cleared have access to the data in the system.

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.

Participant/member contact information is retained until the member terminates their participation in the program or until a particular contact is replaced by another individual. Members' IPM strategy/reporting information is retained until the member organization terminates their participation in the voluntary program.

The EPA Records Control Schedule is NARA 0090 - Administrative Support (Voluntary Programs).

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.

Data are retained for the length of time member organizations remain in the partnership

program. When a member organization withdraws from the program, their information is deleted. Only a small number (currently 3) EPA staff have access to these data.

Privacy Risk:

The length of time the member organizations remain in the voluntary partnership program would equal the length of time we would have to protect the organization's information. There is no records control schedule number that specifically identifies PESP and the software Salesforce that we use to manage and collect members' IPM activities. However, until a special category can be created, PESP's activities and records management fall under EPA's Record Control Scheduler 0090 - Administrative Support Databases (Voluntary Programs) and1012e - electronic software.

Mitigation:

We do not believe an additional records retention category is needed for the PESP Salesforce system but we are open to exploring if an additional category is needed.

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. Information, aggregated from member submissions, is shared through EPA-produced reports and articles with PESP members and stakeholders. Information shared would include program participation (number of members), membership by sector, and information on pest management tactics and IPM outreach being conducted by members.

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

The collected aggregated IPM data is used to develop pesticide usage reports and IPM adoption strategy presentations for senior management (Division Directors, Office Director, and Assistant Administrator) to share with other federal agencies and pesticide stakeholders.

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?

System access is limited to a small number of EPA (OPP/BPPD) staff. External access is not permitted.

4.4 Does the agreement place limitations on re-dissemination?

There are no agreements in place that allow for re-dissemination of the 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:

The collected and aggregated IPM and pesticide data are used to develop reports and presentations for senior Agency management and to share with other federal agencies and pesticide stakeholders. The risk is related to human error.

Mitigation:

The information is protected by access controls which limit it's confidentiality and availability to the authorized borrower. EPA personnel are required to take Annual Security and Privacy Awareness 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?

EPA staff monitor system access to insure only the small number (currently 3) of OPP/BPPD staff are the only persons accessing the system. Chain of command reporting insures that any reports generated from the system are aggregated and division management reviews all presentations, reports, or articles that contain aggregate information from the system.

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

All system users maintain FIFRA CBI clearances, undergo required annual EPA Information Security and Privacy Awareness training, and adhere to other standard Agency training requirements. System users do not receive privacy training specific to the PESP Salesforce account.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

N/A

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 PESP Team authorizes requests for access from users. Account access is setup to limit users 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.

The information collected will allow OPP to leverage the data and technology to achieve the following key goals and/or support:

- Provide OPP with data on Integrated Pest Management tactics and pesticide usage in a variety of agricultural and residential settings.
- Demonstrate the economic benefits related to IPM adoption and implementation.
- Reduce the burden on PESP members who are promoting IPM to other pesticide users and collecting pesticide usage data for their industries.
- Provide PESP member organizations and the program's stakeholders with data on effective IPM techniques to combat pesticide resistance, emerging pest issues and invasive species.
- Promote and track EPA 's contributions to partnerships in key federal initiatives.

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 system allows users (EPA staff) to retrieve information by PESP member (organization) name. The PII of the members' primary and secondary contacts are not used to retrieve member information.

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 goal here is to look at the data collected, how you plan to use it, and to ensure that you have limited the access to the people who have a need to know in the performance of their official duties. What controls have you erected around the data, so that privacy is not invaded? ex. administrative control, physical control, technical control.]

The scope and use of the system was assessed as it was developed resulting in the implementation of user roles that appropriately limit access. Administrative and technical controls limit access to the data collected and how the data are compiled and shared, in summary reports.

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:

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.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

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?

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

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

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16.

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: