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: Certification Plan and Reporting Database (CPARD)	**System Owner: OPP/FEAD**
Preparer: Jeannie Kasi and William Northern	**Office: OCSPP/OPP**
Date: 12/1/2020	**Phone: 703-853-8362**
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:

CPARD is used to house EPA-approved certification plans (CPs) and enable certifying authorities (pesticide State Lead Agencies, Tribes and Federal Agencies with EPA-approved plans) to fulfil annual reporting requirements. CPRAD is used to identify all certifying authorities to readily access information on certification programs administered by other jurisdictions and it an external facing system with public data.

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?

7 U.S.C. §136 et seq. (1996) FIFRA Section 23 and 40 CFR 171 require pesticide SLAs, Tribes and Federal agencies to have EPA-approved certification plans, keep them updated, and submit revised plans to EPA by March 4, 2020. The regulations at 40 CFR 171 require these same agencies to report annually on the number of applicator certification totals.

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?

September 19, 2020 (extension granted) to December 19, 2020

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.

The OMB Control No. for this collection of information is 2070-0029. EPA 0155.

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?

No. The data is hosted in the NCC Data Center. No Cloud Service Provider is needed.

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).

CPARD contains EPA-approved pesticide applicator plans categorized as state, tribes, territories and federal plans. Plans contains information for each certifying entity – which is a state, tribe, territory or federal government entity (e.g., name, address, telephone number, email address, company name and organization).
Also holds;

· Laws and regulations (pdf or hyperlink)
· Other government and university entities with whom they cooperate
· Types and categories of pesticide applicators certified in their program
· Requirements for pesticide applicators for certification and recertification
· Administrative practices of the government entity

· Numbers of pesticide applicators certified and recertified each year by type and category
-Tracking status of EPA reviews of revised certification plans
-List of Questions and Answers
-Support documents

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

EPA inputs the tracking status of EPA reviews of revised certification plans, Questions and Answers, and supporting documents.

The State Lead Agency, Tribe or Federal Agency enter the number of applicators certified and recertified each year. They can also edit changes to contact information.

The rest of the information usually remains static (the same) from year to year. If there is a change, EPA will change it for them.

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

No.

2.4 Discuss how accuracy of the data is ensured.

Much of the information remains static from year to year. EPA reviews and quality checks the number of certified applicators reported annually. EPA inputs the information for tracking, questions and answers, and supporting documents.

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 risk that data may be accessed by unauthorized users or intentionally or un-intentionally exfiltrated.

Mitigation:

The system security plan outlines system level security controls in place to mitigate associated risks: Access Control (AC)-System access is limited to personnel with a need-to-know and Audit (AU)-system access is recorded and logged, administrative accounts are routinely reviewed and

disabled if inactive. Enterprise/common controls are in place to monitor, detect and respond to the exfiltration of user data: Incident Response (IR) and System and Information Integrity (SI).

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?

Yes. Registered state government users (Read only access) can only see tracking information for their state. EPA Regional staff registered users (Read and Write access) can edit and view only tracking information for States in their Region; and can enter information for Questions and Answers. There are three levels of access. 1. CPARD Admin 2. Registered State Gov. 3. EPA Regional staff.

Anybody who wants to log into CPARD has to register in EPA's web application access (waa). EPA approves or rejects registrations. If approved, EPA adds them to CPARD as a user with the i.d. generated in waa.
https://wamssoprd.epa.gov/oam/server/auth_cred_submit?request_id=-6286575994969808699&authmethod=FORM

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

Access controls will be documented in OMS SSP – EIAM/WAM

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

Yes – EPA regional staff are given access to the tracking and Question and Answer sections of CPARD, after their registration is approved in waa.

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?

EPA/Office of Pesticide Programs/Field and External Affairs Division/Certification, Worker Protection Branch; EPA Regional office staff in the pesticide program; representatives of pesticide State Lead Agencies (state government) who are involved in the applicator certification program, and the contractor CSRA whom have the appropriate FAR clause in place.

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.

EPA will retain the EPA-approved Certification Plans and annual applicator certification numbers indefinitely because they are required by FIFRA Section 23 and 40 CFR 171.

EPA will retain the information on tracking, Questions and Answers, and supporting documents until sometime after March 4, 2022 when EPA must have approved all revised Certification Plans. The information will be needed for our office measures (e.g., GPRA).

This is being added to the EPA Records Schedule Number 0090 "Information Tracking Systems."

The electronic software program is to be kept as long as needed to ensure access to, and use of, the electronic records throughout the authorized retention period to comply with 36 CFR Sections 1236.10, 1236.12, 1236.14, and 1236.20. NARA regulations require that electronic records be retrievable and usable for as long as needed to conduct Agency business and meet NARA-approved disposition. The electronic software program is covered by schedule 1012, item e.

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:

The longer records are retained the greater the likelihood data may be accessed by unauthorized users or data may be intentionally or un-intentionally exfiltrated.

Mitigation:

Data records are disposed of in accordance with EPA's record schedule 0090 retention requirements. The system security plan outlines additional system level security controls in place to further mitigate risk: Access Control (AC)-limits access to personnel with a need-to-know and Audit (AU)-system access recorded and logged, administrative accounts are routinely reviewed and disabled if inactive. Enterprise or common controls are in place to monitor and respond to the exfiltration of user data: Incident Response (IR) and System and Information Integrity (SI).

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.

EPA-approved Certification Plans and annual certified and recertified applicator totals are available for public view, without signing into CPARD.

Registered users of state government (pesticide State Lead Agencies) can sign in and enter their own annual applicator totals reports. These state government users are registered in waa and can only log into CPARD after their registration has been approved and the CPARD administrator has added them to the list of users in CPARD.

The other parts of CPARD (tracking, Questions and Answers, supporting documents) are not available for public view. Only users who are registered (State government and EPA staff) can see it after they log in. The tracking information is there for users to see the status of EPA review and approvals of revised Certification Plans.

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

All information is either required in FIFRA Section 23 and 40 CFR Part 171, or pertains to the requirements. Pesticide State Lead Agencies are required to have an EPA-approved Certification Plan and submit annual reports of applicator certification and recertification totals to EPA

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?

This is controlled by giving access to only certain parts of CPARD to registered users only. Registered state government users can log in to report annual applicator totals to EPA. Registered EPA regional users can log in to enter tracking information and Questions and Answers. All information can be accessed and edited by two EPA User Administrators. There are no agreements or MOUs. Most of the information can be viewed by the public – except the tracking information, Questions and Answers, and supporting documents.

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:

There is risk associated with the sharing of information that the information may be shared with unauthorized users or information may be intentionally or un-intentionally exfiltrated.

Mitigation:

The EIAM/WAM and CPARD implement preventative measures to mitigate the above risk, by ensuring that users are properly vetted, and accounts are managed according to Agency, FISMA and NIST. These user accounts are reviewed and managed annually based on the Agency requirements.

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?

State, tribe, territory or federal government must review and fulfill annual reporting requirements. CPARD employ the least privilege and need to know concepts for all users, therefore users can only update their respective plan and data.

.

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

All EPA staff are required to take annual mandatory information security and privacy awareness training and adhere to other standard Agency training requirements. System users do not receive privacy training specific to CPARD.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Lack of or failure of auditing and accountability controls increases the likelihood that data may be accessed by unauthorized users or data may be intentionally or un-intentionally exfiltrated.

Mitigation:

The system security plan outlines system level security controls are in place: Access Control (AC)-limits access to personnel with a need-to-know and Audit (AU)-system access recorded and logged, administrative accounts are routinely reviewed and disabled if inactive. Enterprise or common controls are in place to monitor and respond to the exfiltration of user data: Incident Response (IR) and System and Information Integrity (SI).

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.

CPARD use the information to record the identity and certification status of pesticide applicators certified by EPA. CPARD provide the state, tribe, territory or federal government the ability to manage the EPA-approved certification plans.

.

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.*)

"User can retrieve data on the following fields subject area, topic, and question."

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?

Annually, system personnel: review the Privacy Impact Assessment, perform a risk assessment and undergo an independent security assessment that evaluates system security controls including privacy controls. The system only presents data that is already made available by the Agency. The data is used to develop a risk profile for the Agency based upon the CPARD application data elements.

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 risk associated with the unauthorized use of information.

Mitigation:

An Annual security assessment is conducted to determine the efficacy of implemented security controls. Additionally, the CPARD application regularly performs continuous monitoring activities to include configuration management settings audit and vulnerability scanning. A plan of actions and milestones (POA&Ms) is maintained to manage findings identified during these and other continuous monitoring activities.

***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: