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: Federal Lead-based Paint Program (FLPP) Database System	
Preparer: Robert Wright Robert Wright (Federal OPPT contact)	**Office:** EPA/OCSPP/OPPT
Date: 6/24/2020	**Phone:** (202) 566-1975
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:

EPA administers the certification and accreditation of lead-based paint and renovation, repair, and painting programs in States, Tribal areas and territories that do no have EPA's authorization to independently administer such programs. Under the Federal Lead-Based Paint Program (FLPP), applicants' interest in receiving certification and/or accreditation must submit a complete application package to EPA which includes the appropriate supporting documentation needed to meet the requirements for certification and accreditation and pay any required fees. Also, certified firms must notify EPA of any abatements, they will perform and accredited Training Providers must notify EPA when they will give training classes (pre-notification and workers that they have trained (post-notification).

The FLPP database system supports the application process for the accreditation of training providers and the certification of firms and individual who perform abatement and renovations, repair and painting activities. The FLPP database receives applications (via data entry into database system or online using EPA's Central Data Exchange (CDX)), manages the workflow, develops data-driven letters, and certificates for individual applicants. Training providers, firms and individuals can submit their applications online using CDX and pay required fees using Treasury's Pay.gov. Also, firms and training providers can submit their abatement, pre-training and post-training notifications using CDX. Renovations and Repair Program (RRP) post-training notifications require a picture of workers trained and can be submitted in the post-training notification using CDX. The FLPP database was developed using ColdFusion MX10 for the public tool and Java (Tomcat) as the tunnels to the Oracle (OFM) database. The database is hosted on a cluster of VM servers at EPA's National Computer Center in Research Triangle Park, NC.

On February 22, 2019, and amendment to the FLPP's System of Records was published in the *Federal Register* (Vol. 84, No. 36) to update the category of uses to add lead-based paint and renovator professional' photographs, to add names of training program managers and principal course instructions as well as their education or experience or training qualification, and to discuss EPA's Central Data Exchange (CDX) interconnection or online applications and notifications submissions and other administrative updates to the "Federal Lead-Based Paint Program System of Records" (FLPPSOR).

OMB Memo 14-03, requires Federal agencies to manage information security risks on a continuous basis, including a requirement to monitor the security controls in Federal information systems and the environments in which those systems operate. Current capabilities deployed at EPA include credential management (CRED), configuration settings management (CSM), hardware asset management (HWAM), privileged access management (PRIV), software asset management (SWAM), and vulnerability management (VUL).

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?

- OMB Directive 14-03 requires Federal agencies to manage information security risks on a continuous basis (every 72 hours), including a requirement to monitor the security controls in Federal Information systems and the environments in which those systems operate.
- 44 U.S.C. § 3506, which establishes federal agencies' responsibilities for managing information resources and 40 U.S.C. § 11315, which establishes the responsibilities of the agency's Chief Information Officer to manage agency information resources.
- Federal Information Security Modernization Act 2014 (FISMA) requirement for ongoing system security and is the means by which an organization shows due diligence in providing adequate security for its information and systems.
- The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, that establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

- 40 CFR part 745 Lead--Requirements for Lead-Based Paint Activities in Target Housing and Child-Occupied Facilities.
- 40 CFR part 745 Lead—Renovation, Repair, and Painting Program.

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, a complete system security plan is maintained in EPA's governance risk and compliance tool (Xacta). The ATO expires on July 15, 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.

Yes. EPA ICR No. 1715.10, OMB Control Number 2070-0155.

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

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 FLPP database system collects individuals' names, addresses, telephone numbers, dates of birth, photographs of lead-based paint and RRP professionals, signatures, course test scores, submitted fees, and certificate numbers as well as the names of training program managers and principal course instructors as well as their education or experience or training qualifications. Information is obtained from individuals who have submitted a certification application and have been trained by an accredited training provider. The FLPP database uses the post-training notifications submitted by accredited training providers to show individuals have been trained in the following disciplines: inspectors, supervisors, risk assessors, project designers, abatement workers, renovators, and dust sampling technicians. The FLPP database uses the information to certify abatement program individual's applicants and to show individuals have been certified under the RRP program. The FLPP database maintains information on individuals derived from sources relating to individuals applying for certification and being trained to perform lead-based paint and RRP activities. Also, the FLPP database maintains records of the names of training program managers and principal course instructors as well as their education or experience or training qualifications. The FLPP database disseminates the information to Headquarters and Regional FLPP database user to process applications, generate letters and

certificates, data searches, analysis data, develop reports as well as to support other EPA offices as needed. Outlined in the table below are the FLPP database data elements for the Abatement and RRP programs:

Table 1 FLPP Database Data Elements

FLPP Database Data Elements	Key Identifier
Abatement Program	
Application ID	✓
Applicant ID	✓
Applicant Title	
Applicant First Name	✓
Applicant Middle Name initial	
Applicant Last Name	✓
Applicant Previous and/or Maiden name(s)	
Applicant Phone number	✓
Applicant Alternative contact number	
Applicant Home Address (line 1)	✓
Applicant Home Address (line 2)	✓
Applicant Home City	✓
Applicant Home State	✓
Applicant Home ZIP	✓
Applicant Address for Correspondence or badge certificate	
Applicant Date of Birth	✓
Applicant Date Signed	✓
Applicant Signature Image	✓
Applicant Passport Image	
Applicant Passport Photo Image	✓
Applicant Submitted Fees	
Applicant Exam Test Scores	
Applicant Certification Number	✓
Renovation, Repair & Painting Program	
Training Provider Notification ID	✓
Training Dates	
Training Provider Name	
Training Provider Business Address	
Training Student First Name	✓
Training Student Last Name	✓
Training Student Address	✓
Training Student Date of Birth	✓
Training Student Photo	✓
Training Provider’s Training Manager	
Training Provider’s Training Manager’s Signature	
Training Provider’s Training Manager’s Signature Date	

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

The FLPP database uses EPA's Central Data Exchange (CDX) for applicants to develop their application and pay any required fees to the Department of Treasury's Pay.gov system. CDX then uploads the application and uploads that fees were paid to the FLPP database. Applicants who fails CDX's identity verification process must submit an Electronic Signature Agreement (ESA) to the Agency. Upon receipt and processing of an ESA, then allows the application to be uploaded to the FLPP database for review and processing. Accredited training providers develops post training notices of workers trained and upload the post training notice using CDX. Training providers must submit a photo of workers trained and certified under the RRP program and can use CDX to submit photos. Training providers also have the option of submitting post-training notices via faxes or mail. Post-training notices submitted via faxes or mail will be data entered into the FLPP Database.

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.

Data is reviewed by EPA's Lead program Data Entry Contractors who performs a quality control review of the data uploaded from CDX or data entered by the Data Entry Contractors for accuracy. Detected data anomalies are reported to the FLPP database team and corrected for the FLPP database.

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?

Administrative access is granted only to qualified, trained individuals with a need-to-know. These users are granted access privileges based on their user role and their accounts are regularly reviewed and audited. All administrative system actions are logged in accordance with audit security controls. Limited read-only user access is granted as well on need to know basis.

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

EPA access control procedures outlined in CIO 2150-P-01.2 and are located here https://www.epa.gov/sites/production/files/2015-09/documents/cio-2150-p-01.2.pdf . System specific implementation of access controls are outlined in the system security plan.

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?

A subset of EPA personnel and EPA contractors a need to know may be granted read-only access to the FLPP database via the Agency WAM access. Administrative access is limited to authorized EPA personnel and EPA contractors. External parties are not permitted administrative or elevated privileged access to the FLPP database data.

EPA mandates the inclusion of FAR clauses in EPA service contracts.

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.

FLPP database data is refreshed at frequency less than or equal to 72hrs. Data may be retained as a result of system backups provided by the EPA hosting facility. System backups are retained for a period not to exceed 365-days. The FLPP database system complies with EPA Records Schedule 0089.

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 0089 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.

No.

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

N/A.

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?

N/A.

4.4 Does the agreement place limitations on re-dissemination?

N/A.

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. Information is not shared externally.

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 as stated in Section 6.1?

The system attempts to limit the misuse of information by first controlling access to the data. Access to data is limited to those with a demonstrated need to know and controlled by role assignment. The Agency has in place controls that limit the exfiltration of data further mitigating the likelihood of data misuse. System audit controls are also in place to record user actions relating to data use.

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

All EPA Government Employees and contractors must complete EPA's Annual Information Security and Privacy Awareness Training. In addition, all users are required to read and sign the EPA Rules of Behavior that governs the appropriate use of information systems. Training is accessible via the Agency's FedTalent training web site.

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.

EPA uses the data for processing applications, analyzing information, generating letters and reports, and providing information to allow for executing various enforcement actions. The data will be used to certify individuals and firms to conduct lead-based paint and renovation, repair and painting activities, accredit training providers to conduct lead-based paint and renovation, repair and painting activities training and gauge compliance with program requirements.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes _X__ No ___. 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.)

Yes, the information is retrieved by Application ID or Applicant ID for individuals under the abatement program and the information is retrieved by training provider notification ID for individuals under the RRP program. Application ID and provider ID are linked to the individual. **EPA-54**

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 FLPP database 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 use of information that the information may be accessed by unauthorized users or information may be intentionally or un-intentionally exfiltrated.

Mitigation:

An Annual security assessment is conducted to determine the efficacy of implemented security

controls. Additionally, the FLPP database 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.

Applicants applying online using EPA's CDX tool see the Privacy Act Statement which informs them of the following: The information collected on this form will be used to establish the applicant's eligibility for certification to conduct lead-based paint activities in target housing and child occupied facilities.

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?

Disclosure of the information is voluntary, however, the failure to provide this information may delay or prevent an applicant's certification.

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:

There is risk associated with the notice provided by unauthorized users or intentionally or un-intentionally exfiltrated. The Privacy Act Statement informs of how the data will be used and is consistent with the stated uses.

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 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 can amend their application form at any time with new or updated information on themselves. Also, an individual can file a Freedom of Information Act request to obtain information.

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

Individuals who identify inaccurate or erroneous information can amend their application form with new or updated information and the updated information will be reviewed and updated in the FLPP database.

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:

None, there is a proper procedure in place related to redress.

Mitigation:

None.