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: Office of Pesticide Programs Local Area Network General Support System (OPP LAN GSS)	**System Owner: Jan Krysa**
Preparer: William Northern	**Office: OCSPP/OMCO/ITSD/ISB**
Date: 01/29/2026	**Phone: 202-566-1493**
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:

The OPP LAN is only accessed by OPP Personnel and support contractors. The OPP LAN does not collect data. Outside/public access is restricted. The boundary of the OPP LAN GSS is a network firewall which is managed by the EPA Office of Finance and Administration (OFA). All internet connections, EPA Wide Network Infrastructure, desktops, and VoIP based telephones are managed by OFA and are considered outside the scope of the OPP LAN GSS. Answers to the sections below refer to the subsystem PRISM MA.

Subsystem: Pesticide Registration Information SysteM Major Application (PRISM MA)

PRISM as a subsystem of the OPP LAN GSS collects PII. The OPP GSS LAN is host to the Pesticide Registration Information SysteM Major Application (PRISM MA) which processes Controlled Unclassified Information (CUI) as regulated by the Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA). Statutory basis for EPA's pesticide program includes provisions, under which certain information is protected and released, and penalties for unauthorized disclosure of protected information by federal and contract employees. Controlled Unclassified Information (CUI) is any information received by EPA from any private source or public agency that contains trade secrets or commercial/financial information that has been claimed as confidential by the person submitting it and which has not been legally determined to be non-confidential by the EPA General Counsel. FIFRA requires the EPA to protect CUI obtained under the Act from public disclosure and imposes criminal penalties for the willful or negligent unauthorized release of such information.

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?

The Federal Food, Drug, and Cosmetic Act (FFDCA), the Federal Fungicide, Insecticide, and Rodenticide Act (FIFRA), and The Pesticide Registration Improvement Act of 2003 (PRIA) and subsequent reauthorizations determine and document the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of the OCSPP/OPS mission.

Authority is reviewed and approved by Office of General Counsel (OGC).

Authority for collection is published in Federal Insecticide, Fungicide, and Rodenticide Act, 7 U.S.C. §136 et seq. (1996) as amended and the Federal Food, Drug, and Cosmetic Act 21 U.S.C. §301 et seq. (2002)

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?

The OPP LAN SSP is under review and is in the process of being issued an Authorization-to-Operate. **The ATO expires July 31, 2026**

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.

There is no information collected that is covered by the Paperwork Reduction Act.

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).

- **PRISM/Pesticide Submission Portal collect:**
  - Submitter's name and organizational contact information (company name, company address, company phone, email address, etc.).
- **PRISM/Label Use Information System (LUIS) collect:**
  - EPA Staff names.
- **PRISM Business Objects Reports collect**:
  - EPA staff names.
- **PRISM Chemical Search collect:**
  - EPA staff name
  - work email
  - work phone
- **PRISM Document Repository/e-Registration Workflow collect:**
  - Names.
- **PRISM e-Studies Module collect:**
  - Study author name(s).
- **PRISM, e-Submission Module collect:**
  - Registrant contact name, email address, phone number
  - Documents carried through the e-submission module may contain names, email addresses, phone numbers
- **PRISM Incident Data System (IDS) collect:**
  - Type of incident
  - Product information
  - Aggregate and individual incident reports
- **PRISM OPSIN Data Entry and Query Modules collect:**
  - EPA staff name, work email address, work phone number, workforce ID, LAN ID
  - Company contact name, business phone number, business email
- **PRISM Public Health Tracking System (PHTS) collect:**
  - Names
- **Pesticide Product and Label System (PPLS) collect:**
  - EPA employee name in PDFs

- **PRISM Registration Review/EDSP collect:**
  - Registrant names, email addresses
  - EPA employee names
- **PRISM State Label Issue Tracking System (SLITS) collect:**
  - EPA employee names, email addresses
  - Federal and State enforcement personnel names
- **PRISM User Contract Management (UCM) module collect:**
  - EPA staff and persons with FIFRA CBI clearance names,
  - email address,
  - work phone
  - workforce ID
  - contractor information
  - contract / work order numbers
- **OPS PRISM Web Applications collect:**
  - First & Last Name
  - EPA Office Phone Number
  - EPA Email Address
- **PRISM/Endangered Species Knowledge Base (ESKB) collect:**
  - Names
  - email addresses
  - phone numbers of EPA staff and external stakeholders

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

Most of the data is entered manually into PRISM, some data is pulled from EPA's Active Directory system (AD) (EPA Staff) and EPA's Central Data Exchange (CDX) (Business Community) data is pushed to PRISM.

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 collected from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

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:

Minimal. Most of the information is already available to the public.

Mitigation:

PII that is not already public is restricted to authorized EPA employees.

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?

Individual Modules limit access of data to specific user groups based on business function and need. System functionality is controlled by roles assigned to individuals or groups of individuals. EPA staff are required to have current FIFRA CBI status in affect to access PRISM. Access is granted to specific Modules only after completing a PRISM System Access form. Registrants access the CDX only after completing the registration process. Public-facing modules (Chemical Search, PPLS) contain only data considered public information and do not require user authentication.

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

Access is granted to specific Modules only after completing a PRISM System Access form. Registrants access the CDX only after completing the registration process. EPA staff and contractors do not have access to registrant passwords. This ensures the integrity of content submitted to the Agency. Read access is managed via roles and may (for internal modules) require FIFRA CBI clearance to be current.

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?

Information in PRISM is available to internal and external parties with the appropriate user ID, permissions, and roles. This includes contractors. The following FAR clauses are included in the contract: 24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act.

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.

PRISM is scheduled under EPA Record Schedule 0329 (permanent) and CDX under 0097 (3 years).

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:
Due to length of time that PRISM data is retained there could be a privacy risk if data is not handled, stored or disposed of properly.

Mitigation:
Ensure that all persons that need access to PRISM have had the proper FIFRA CBI training and clearances, that all sensitive material is properly handled and stored.

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. Some information in PRISM is shared outside of EPA via public search pages. 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.

Sharing provides transparency to external stakeholders and the public of EPA's pesticide regulatory process. 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?

The PRISM system owner reviews and approves, on a case-by-case basis, information sharing agreements and understandings. PRISM does not control how data are used outside of EPA-managed applications.

4.4 Does the agreement place limitations on re-dissemination?

No

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 no information sharing or information sharing partnerships with the data stored within PRISM.

Mitigation:

There is no information sharing or information sharing partnerships with the data stored within PRISM.

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 Pesticide Programs monitors the design, maintenance, administration, and use of PRISM for adherence to security and privacy standards. OPS holds a Conceptual Review of each PRISM module as it is being architected and designed. OPS reviews the modules 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 module and its users. OPS holds an Architectural Review of the module once it has been designed in detail, to assure that PRISM'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.

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

Privacy training is part of the Agency's Annual Information Security and Privacy Training requirements. PRISM users are trained in the proper management of confidential information.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

The risk exists that PRISM being hosted on the OPS LAN could have inadequate privacy controls at the application level, not taking sufficient advantage of the controls provided by the OPS LAN.

Mitigation:

In conducting Conceptual Review, Design Review, and Production Readiness Review for PRISM, OPS reinforces that the application must have sufficient privacy auditing and accountability controls in place.

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.

PRISM supports the mission of OPS in managing the registration of pesticide products and ingredients. To support this mission, external contact information is required to provide for efficient interactions and transparency with external stakeholders and the public.

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.*)

Informational access is managed using internally assigned usernames in combination with two-factor authentication and active user CBI status. Usernames are not distributed outside the Agency. OFA manages the assignment and retirement of employee and contractor usernames currently done through the Active Directory system. Read access is managed using administrator-managed system user accounts and the module-by-module access assignment as specified in Section 3.1. Some PRISM modules, for example, the PRIA Renegotiation Module include user-facing logs including username used to track approval chains. Work-flow modules include sender and receiver usernames only. PRISM has no direct connection to OHR-managed systems containing PII data. Usernames, organization, work telephone number and physical location, and title may be pulled from Active Directory, stored and displayed. No additional PII is stored or displayed by PRISM modules. System data may be queried by many possible metadata elements including chemical name, chemical PC code, CAS number, registration number, Registration Review case number.

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 PRISM application resides on the OPP LAN GSS within the Office of Chemical Safety and Pollution Prevention. This GSS has an ATO compliant with SP 800-53 security controls and EPA security standards. The application itself has access controls in the form of required logon and prior authorization is required to obtain an account.

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:

Privacy risk could be introduced if users of PII are not correctly trained and informed about disclosure and handling procedures.

Mitigation:

Ensure that all users of PRISM have the proper ISAPT Training, have signed the EPA National Rules of Behavior, and have completed the FIFRA CBI Briefing and have the proper clearance.

***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 OPSortunities 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 OPSortunity 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:

I attest as the Agency Privacy Officer that **AR-2 OCSPP OPP LAN** Privacy Impact Assessment (PIA) has been reviewed. The privacy implications have been adequately identified with appropriate mitigation statements included for implementation in the development or use of information technology systems.

Respectfully,

ROBERT KELLY

Digitally signed by ROBERT KELLY
Date: 2026.05.08 14:25:21 -04'00'

Lee Kelly
Agency Privacy Officer
Cybersecurity Planning & Risk Mgmt Branch
EPA/OFA