United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev 2/2026 – 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 Roster.docx

System Name: Office of Pesticide Programs Local Area Network General Support System (OPP LAN GSS)		**System Owner:** Jan Kyrsa	
Preparer: William Northern		**Office:** OCSPP-OMCO-ITSD	
Date: 04-24-2026		**Phone:** 202-566-1493	
Reason for Submittal:			
New: ☐	Revised:☐	**Annual Review: X**	Rescindment: ☐
System Lifecycle Stage(s):			
Definition: ☐	Development/Acquisition: ☐	Implementation: **X**	
Operation & Maintenance: **X**	Rescindment/Decommission: ☐		

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. 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 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?

Yes. The OPP LAN GSS Authority to Operate (ATO) is current and expires on February 25, 2027**.**

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.

No. PRISM does not collect information subject to the Paperwork Reduction Act; it relies on existing regulatory submissions and internal records rather than PRA-covered information collections.

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. PRISM data is not maintained or stored in a cloud; it resides on the OCSPP/OPP LAN GSS. Accordingly, no CSP is used, FedRAMP does not apply, and no cloud service model (PaaS/IaaS/SaaS) is involved.

Section 2. 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).

- Names (submitters/registrants, EPA staff/employees, enforcement personnel, study authors, external stakeholders)
- Contact information: email addresses; phone numbers (work/office/business)
- Organizational/company details: company name; company address
- Workforce/system identifiers: Workforce ID; LAN ID
- Contractor and contract details: contractor information; contract/work order numbers
- Incident and product data: incident type; product information; aggregate and individual incident reports
- Documents/records that may contain names, emails, and phone numbers (e.g., PDFs and e-submission documents)

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

Most data in PRISM is entered manually by users. EPA staff information is pulled from EPA Active Directory (AD), while Business Community data is provided via the Central Data Exchange (CDX) and pushed into PRISM through established integrations.

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 enforced through documented SOPs, structured data curation workflows, and moderated crowd-sourced contributions. Automated validations and periodic review checkpoints help prevent and correct errors. Row-level audit trails capture who made what change and when (timestamps, user IDs, before/after values), and record-level versioning supports archival, traceability, and rollback.

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 privacy impact. The data is primarily professional contact details and regulatory records that are already publicly accessible (e.g., product and label information). It does not include sensitive personal identifiers (such as SSNs or DOB). Limited non-public elements (e.g., internal workforce/LAN IDs, contract/work order numbers, and any CBI) are access-restricted and monitored, further reducing residual risk.

Mitigation:

Non-public PII is accessible only to authorized EPA employees under least-privilege, role-based access controls, with multifactor authentication, encrypted storage and transmission, and continuous monitoring/audit logging. Access is granted via documented approvals, reviewed periodically, and revoked when no longer needed. Handling follows established SOPs and CBI procedures; external sharing is prohibited without formal authorization, and violations are subject to disciplinary action.

Section 3. 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?

Access is enforced at the module level with role-based controls to ensure least privilege by business function; roles assigned to individuals or groups determine available features and data. EPA staff must maintain current FIFRA CBI clearance to access PRISM, and access to specific modules is granted only after approval of a PRISM System Access form, with periodic reviews. Registrants access PRISM via CDX only after completing CDX registration, while public-facing modules (e.g., Chemical Search, PPLS) contain only public information and require no authentication.

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

Access to PRISM modules is provisioned only after an approved PRISM System Access form and periodic review. Registrants access PRISM via CDX after completing CDX registration; PRISM neither stores nor exposes registrant passwords, so EPA staff and contractors cannot view them, preserving submission integrity. Read access is role-based, aligned to least privilege and business need, and internal modules may require current FIFRA CBI clearance.

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

No. PRISM does not include additional components with separate role assignments or responsibilities; all access and duties are governed centrally through PRISM's role-based model and module permissions. External integrations (e.g., AD, CDX) supply data but do not introduce distinct PRISM roles.

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 accessible to authorized internal users, external stakeholders, and contractors with valid user IDs and role-based permissions aligned to least-privilege and need-to-know. Contractor access is governed by FAR 24.104 and the Privacy Act clauses 52.224-1 (Privacy Act Notification) and 52.224-2 (Privacy Act), which mandate compliance with federal privacy requirements.

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 retains registration and registration review data and documents permanently; inactive records are closed at completion of action and transferred annually to the National Archives after any audits, together with system documentation, per EPA Records Schedule 0329 (N1-412-09-16c, h). Other components—software, inputs, reference/information-tracking databases, and outputs/reports—are temporary and disposed of under the applicable NARA authorities (e.g., N1-412-09-16a; DAA-0412-2013-0009; EPA 0088/0089), destroying them when no longer needed to support access and use throughout the authorized retention period. These retention requirements support statutory and program needs under FIFRA, FQPA, and PRIA, ensuring reliable analysis, traceable decisions, and preservation of critical regulatory records while providing public access to non-CBI information.

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 long retention period increases the exposure window for unauthorized access or inadvertent disclosure if PRISM records, especially non-public PII and FIFRA CBI, are not consistently protected, monitored, or destroyed per schedule.

Mitigation:

Enforce least-privilege, role-based access with current FIFRA CBI training/clearance; require MFA and encryption in transit and at rest; follow SOPs for handling, retention, and disposal under EPA Records Schedule 0329; maintain row-level audit logs and continuous monitoring; conduct periodic access recertification and training; and perform NARA/EPA-compliant secure destruction of sensitive records at end of life.

Section 4. 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 governments, 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. PRISM publishes selected data to external audiences via public search pages (e.g., Chemical Search, PPLS), and only non-confidential, publicly releasable information is exposed; CBI and non-public PII are excluded and remain access-controlled internally.

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

Sharing enhances transparency into EPA's pesticide regulatory process for external stakeholders and the public. Under FIFRA security requirements, external access to non-public information is rare and permitted only under narrowly defined conditions with Administrator-level approval. Authorized officials manage FIFRA security procedures to ensure any access is purpose-bound and compliant with statutory requirements.

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 information-sharing arrangements (e.g., MOUs, ISAs, data use agreements) on a case-by-case basis to ensure compliance with legal and policy requirements. Once data are released outside EPA-managed applications, downstream use is governed by recipient policies and applicable law; PRISM does not manage or enforce external use beyond stated terms and access controls.

4.4 Does the agreement place limitations on re-dissemination?

No. The agreements do not impose limitations on re-dissemination; once public, non-confidential data is shared, recipients manage further distribution under their own policies and applicable law.

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 from external sharing, as PRISM does not share non-public data or maintain information-sharing partnerships.

Mitigation:

Maintain the no-sharing policy for non-public data, limit exposure to public, non-confidential information only, and enforce role-based access, current FIFRA CBI clearance, and auditing.

Section 5. 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?

OPP oversees PRISM's design, maintenance, administration, and use to ensure compliance with security and privacy standards. OCSPP/OMCO applies a three-stage governance process: Conceptual Review (architecture, data entities and relationships, user communities, roles and responsibilities, licensing, shared objects, and data-use restrictions), Architectural Review (conformance of detailed design to the approved concept and restrictions), and Production Readiness Review (verification of testing and compliance before deployment). The system owner must attest to all data-use restrictions and ensure they are enforced within the module and by its users. Ongoing monitoring and periodic reviews confirm continued adherence.

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

PRISM users complete the Agency's annual Information Security and Privacy training, supplemented by module-specific instruction on handling confidential information (e.g., FIFRA CBI and PII), least-privilege access, SOPs, and incident reporting. This ensures consistent, compliant management of sensitive data across the system.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Discuss the privacy risks associated with the technical and policy-based safeguards and security measures. How were those risks mitigated?

Privacy Risk:

Hosting PRISM on the OPP LAN can create gaps if application-level privacy controls do not fully leverage LAN security, resulting in inadequate role enforcement, logging, or encryption.

Mitigation:

OCSPP/OMCO requires app-specific privacy controls through Conceptual, Architectural, and Production Readiness reviews, mandating integration with LAN security (e.g., AD-based roles, MFA), least-privilege RBAC, encryption, comprehensive audit logging, continuous monitoring, and periodic control assessments.

Section 6. 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

List each use (internal and external to the Department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used. If Social Security numbers are collected, state why the SSN is necessary and how it was used.

PRISM uses regulatory and contact information to manage pesticide registrations and reviews, track workflows and decisions, process submissions, and publish non-confidential data for transparency. External contact details enable authenticated communications with registrants and stakeholders (e.g., notifications, coordination, inquiries), supporting timely regulatory actions and public access to approved information. Access and use are limited to mission needs under role-based controls and applicable FIFRA/CBI requirements.

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 enforced with internally assigned Active Directory usernames, multifactor authentication, and current FIFRA CBI status; EAIM provisions and retires employee and contractor accounts via AD, and usernames are not shared outside the Agency. Read access is role-based and administered per module (see Section 3.1), with audit trails: user-facing logs (e.g., PRIA Renegotiation) record usernames in approval chains, and workflow modules capture sender and receiver usernames only. PRISM has no direct connections to OHR systems containing PII; it may display limited directory attributes (username, organization, work phone, physical location, title), and no additional PII is stored. System data can be queried by multiple metadata elements, including chemical name, PC code, CAS number, registration number, and 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 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.

PRISM operates on the OPP LAN General Support System (GSS) with a current Authority to Operate, implemented in accordance with NIST SP 800-53 and EPA security standards. Application controls include AD-integrated authentication, multifactor login, role-based

authorization, and accounts provisioned only after prior approval. Access is logged and monitored, and data is encrypted in transit and at rest consistent with GSS baselines.

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:

Inadequately trained users may mishandle or improperly disclose PII.

Mitigation:

Require annual ISAPT training, a signed EPA National Rules of Behavior, and current FIFRA CBI briefing and clearance; enforce least privilege, role-based access, multifactor authentication, and periodic access reviews with monitoring.

If no SORN is required, STOP HERE.

The National Privacy Program (NPP) will determine if a System of Records Notice (SORN) is required. If so, the following additional sections will be required.

Section 7. 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. 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 Freedom of Information Act (FOIA).

Privacy Risk:

Mitigation:

I attest as the Agency Privacy Officer that **Office of Pesticide Programs Local Area Network General Support System (OPP LAN GSS)** 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: 2026.09.08 11:30:25 -04'00'

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