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: EESD Salesforce Module		**System Owner:** Carissa Cyran	
Preparer: Carissa Cyran		**Office:** AO-OAE-EESD	
Date: 7/22/2026		**Phone:** 240-814-1145	
Reason for Submittal:			
New: ☐	Revised: X	Annual Review: ☐	Rescindment: ☐
System Lifecycle Stage(s):			
Definition: ☐	Development/Acquisition: X	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 Environmental Education and Stewardship Division (EESD), formerly the Office of Public Engagement and Environmental Education (OPEEE), Salesforce module was built within the OCSPP Salesforce System and currently meets the following business need: Record basic information about awarded Environmental Education (EE) grants and track the project results of these awarded grants in terms of EESD's specific goals for this program.

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?

Section 6 of the National Environmental Education Act of 1990 (Public Law 101-619) authorizes the award of Environmental Education grants by EPA. Separately, the authority to gather progress performance for assistantship programs is derived from 2 CFR Part 200, "Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards."

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 EESD Salesforce module resides within the Office of Chemical Safety and Pollution Prevention (OCSPP) Salesforce system as a tenant client and inherits all security controls from the OSCPP Salesforce system. EESD operates its module, including development and O&M, per OCSPP Salesforce governance policies. OCSPP Salesforce has a FISMA Moderate ATO. EESD is not involved the maintenance of OCSPP's Salesforce's ATO. The ATO will expire on May 31, 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.

EESD's EE grants program is covered under EPA ICR No. 2731.01, OMB Control No. 2090-0034. A non-substantive change request was submitted, EPA ICR No. 2731.02, and is awaiting approval.

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?

Data is maintained in the OCSPP Salesforce system, which uses Salesforce's Federal government dedicated servers based in North America per FedRAMP requirements. The Salesforce products that the OCSPP Salesforce system uses are a FedRamp approved SaaS.

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).

Contact object (Shared standard object within OCSPP Salesforce; used by EE Grants)

- Grant recipient representative name Email address
- Office and/or Organizational mailing address

Files (Shared standard object within OCSPP Salesforce; used by EE Grants)

- Grant recipient representative name
- Email address
- Office and/or Organizational mailing address
- NOTE: Due to EPA business need to have the grant final report exist as a file for recordkeeping purposes, the reports may continue to exist to be able to export files that would contain grant recipient representative name, email address, office and/or organizational mailing address.

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

Currently, information is hand-entered by EPA staff. Data is received via email from grant recipients.

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.

Accuracy of the data is maintained by EESD and Regional staff through following up with EE grantees. EESD and Regional staff are the Project Officers for the EE grants. Additionally, EESD staff complete quarterly quality assurance checks to ensure accuracy of data.

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 EE grants program records contact information for grant recipient representatives, including name, email address, and office or organizational mailing address. This creates a privacy risk if reports or exported files contain more information than is necessary for program administration or if contact details are unnecessarily exposed to users who do not need them.

Mitigation:

The system is intended to support post-award tracking of EE grants and unified reporting of grant results, rather than requiring EESD staff to request information that may contain PII data elements via email. The EESD Salesforce module resides within the OCSPP Salesforce system, which uses FedRAMP-approved SaaS infrastructure and inherits security controls including privileged access,

authentication, audit trails, and Salesforce Shield encryption. These controls help reduce the risk of unauthorized exposure of grant recipient contact information.

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?

Yes, the EESD Salesforce module resides within the OCSPP Salesforce system and inherits all security controls from the OSCPP Salesforce system. EESD further operates its module, including development and O&M, per OCSPP Salesforce governance policies. EESD staff do not have any ability to change security-related controls in the system.

EESD does not involve the maintenance of OCSPP's Salesforce FISMA Moderate ATO and is not privy to its security plan documentation; the current system profiles for EESD were established by the contractor which supports all OCSPP Salesforce security, governance, and development. All current users of the EESD module are EPA staff.

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

OCSPP Salesforce security plan and related artifacts.

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

Yes, but these are unrelated to EESD's module. There are multiple modules implemented on the OCSPP Salesforce system for other EPA programmatic needs.

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?

An EPA contractor which supports the production maintenance of the OCSPP Salesforce system has access to the data. EESD does not hold the contract(s) under which this contractor works – which is both an OCSPP contract vehicle and EPA Working Capital Fund. However, both contracts have the appropriate clauses.

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.

The applicable EPA records schedule for EE grants progress and final reports is schedule 1003 (NARA disposal authority DAA-0412-2013-0008-0002.) The EESD

Salesforce module is intended for the post-award tracking of EE grants in terms of grant project accomplishments. It is not intended to duplicate or replace grants management functionality in NGGS and other OGD tracking systems and is therefore not a recordkeeping system for EE grants. In practice, however, there is no intention to delete EE grants data from the EESD Salesforce module so that EESD has a single repository from which to report the results of its EE grants program.

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 OCSPP Salesforce system is maintained with privileged access and with further protection such as Salesforce Shield, which provides system monitoring and data encryption. No actions are performed in the system without authentication, and an audit trail of all logins and actions in the system are produced automatically. We see no privacy concerns related to retention.

Mitigation:

Not applicable due to no privacy concerns.

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.

No data is currently shared directly from the system outside EPA. Data received in the system, such as project summaries, are revised and posted to the EPA website. Aggregate data about EESD's grants program is taken from the system and used for reports.

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

Not applicable. No data is currently shared directly from the system outside 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?

Not applicable. No data is currently shared directly from the system outside EPA.

4.4 Does the agreement place limitations on re-dissemination?

Not applicable. No data is currently shared directly from the system outside EPA.

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:

Not applicable. No data is currently shared directly from the system outside EPA..

Mitigation:

Not applicable. No data is currently shared directly from the system outside EPA.

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?

The OCSPP Salesforce system is maintained with privileged access and with further protection such as Salesforce Shield, which provides system monitoring and data encryption. No actions are performed in the system without authentication, and an audit trail of all logins and actions in the system are produced automatically.

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

All EPA staff users and contractors' complete annual privacy training.

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:

Unauthorized access jeopardizes accountability and puts the following privacy EE grant related information at risk: name, email address, and office or organizational mailing address. 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 OCSPP Salesforce system authorizes requests for access from users. Account access is set up to limit borrowers 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. 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.

The EESD Salesforce module currently meets the business need of tracking the project results of awarded EPA Environmental Education grants in terms of the EESD's specific goals for this program.

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.

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 OCSPP Salesforce system is maintained with privileged access and with further protection such as Salesforce Shield, which provides system monitoring and data encryption. No actions are performed in the system without authentication, and an audit trail of all logins and actions in the system are produced automatically. This information has been collected by years via email and paper by EPA staff that now have access to the EESD Salesforce module. The EESD Salesforce module should improve the protection of PII data by reducing reliance on paper

records, hard-drive downloads, non-secure shared drives, and EPA programmatic inboxes.

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:

Information may only be used for the intended purpose previously described in the "general description/overview" section of this document (page 1). The risk to "uses of information" occurs when information is used for unintended purposes.

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 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 **EESD Salesforce Module** 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: 2026.07.30 14:47:52 -04'00'

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