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: Water Infrastructure Finance and Innovation Act of 2014 (WIFIA) Knowledge Management System	
Preparer: Elinor Keith	**Office: Office of Water – Project Management Office**
Date: 12/1/2020	**Phone: (202) 564-7784**
Reason for Submittal: New PIA__X__ Revised PIA____ Annual Review____ 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 Water Infrastructure Finance and Innovation Act of 2014 (WIFIA) established a federal credit program administered by EPA. WIFIA authorizes EPA to provide loans to eligible water infrastructure projects. Initially, much of the focus has been on loan origination - that is, reviewing loan application materials, performing engineering and underwriting due diligence, developing appropriate loan terms and closing loans. After a loan is closed, WIFIA's portfolio management team leads individual transactions from closing to final maturity (this can be 35+ years). Portfolio management responsibilities are numerous but generally are intended to achieve the following critical objectives:

- monitor portfolio risk and compliance,

- track key loan requirements, information and status,
- process and document disbursements and related accounting actions,
- maintain and document borrower communication, and
- maintain robust loan-specific and portfolio-wide metrics reporting capabilities.

As the portfolio of closed loans grows, the WIFIA program believes an IT system to assist in the portfolio management functions will be essential.

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 33 U.S.C. **3901** Chapter 52, Water Infrastructure Finance Innovation Act (WIFIA) authorizes the operation of this loan 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?

No. A system security plan still needs to be created. It will also have an ATO before becoming operational.

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 ICR required.

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?

Yes, it would be in SalesForce, a FedRamp-approved cloud at a moderate level. The type of service is PaaS provided by the CSP.

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).

Names, titles, business addresses, business phone numbers, and business email addresses for points-

of-contact for each loan

Documents submitted by borrowers, which can contain CBI and account numbers of the borrowing entity (a business or governmental organization; not individuals)

Assessments by EPA of loan compliance, including site reports

Fee, disbursement, and repayment schedules and copies of information from COMPASS (manually input into this system) of what money have actually been disbursed and repaid

All information currently planned to be in the system is used to maintain communications with the borrower, determine ongoing compliance with the terms of the loan, and calculate and keep track of disbursements, fees, and payments.

In the future, the system may also cover the process of potential borrowers submitting a letter of intent and the WIFIA program considering their eligibility for a loan. Information retained during that process would be very similar to that during the lifetime of the loan, but be for potential borrowing organizations. Official loan signature would continue to be managed outside the system.

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

Loan information will be inputted by EPA employees after the loan is signed and ongoing reports (construction reports, changed in the borrowing organization's financial status) will be provided by the borrower. The borrower points-of-contact will need to maintain an account and submit documents showing their loan compliance and any changes relevant to the terms of the loan, such as if an outside loan were taken or the borrower's credit rating changed.

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

The WIFIA team reviews publicly available data and Electronic Municipal Market Access (https://emma.msrb.org/) to assess the financial situation of the borrower. Additionally, they review any of the borrowers' or project's webpages. The system will not directly integrate with these sources.

Bureau of Labor Statistics inflation figures are used in the calculation of fees.

2.4 Discuss how accuracy of the data is ensured.

Borrowers are required to provide accurate information under the terms of the loan agreement. They will be given access to all information they provide to help correct any accidental data entry errors.

Additionally, system testing will confirm the accuracy of calculations.

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 risk comes from unauthorized access to this PII. An unauthorized individual can gain access to this in one of two ways: they actively are able to access the system; or someone who is authorized provides the information to them.

Mitigation:

Information will be maintained in a FedRamp-approved platform with a moderate ATO and annual security assessments will be conducted. Access controls are in place to ensure only those authorized and have a need-to-know may access the data. EPA users are provided annual ISAT and sign RoB.

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?

Borrowers in the system will be limited to viewing information related to their loans. The WIFIA team is small and would all need equivalent level of access to information across the system in order to jointly manage the loan information.

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

In the System Security Plan

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

No, particularly due to limited licenses, the only roles are:

1. WIFIA Team members
2. Loan borrowers

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?

Loan borrowers would have access to information about their own loan. Any contractors would have appropriate FAR language in the contract per EPA policy. EPA WIFIA Team members will have access to the borrowers submission.

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.

1003: Grants and Other Program Support Agreements, see this link, https://intranet.epa.gov/records/schedule/final/1003.html. Records are maintained for 3-, 10-, or 20-years following closure under schedule 1003. They are maintained to establish the borrower's compliance with loan terms.

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:

Contact information is maintained primarily as part of the official record, according to EPA schedules regardless of the continued existence of an organizations change in ownership. The risks are loss of privacy data and the possibility that data is deleted.

Mitigation:

The system controls access to authorized individuals in order to avoid loss of data by requiring users to enter username and password in order to access the system. Accidental deletion of data by authorized users is mitigated by backing the data up so that it can be recovered.

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.

The only information sharing would be on one side with the borrowers to see their own information and with the Treasury managed system COMPASS to process payments.

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

With borrowers: they require access to maintain the information and submit reports

With Treasury: necessary to process payments

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?

None directly (interface with Treasury is via COMPASS); there is no MOU for the use of COMPASS

4.4 Does the agreement place limitations on re-dissemination?

None.

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:

The information is shared with borrowers and potential risks are associated with a borrower's information being made available to the public. The EPA WIFIA Team shares information through manual means, not direct connection to other systems. The risk is related to human error.

Mitigation:

The information is protected by access controls which limit it's confidentiality and availability to the authorized borrower. EPA personnel are required to take Annual Security and Privacy Awareness Training.

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?

Borrowers are required to submit specific information That the WIFIA team members need to process and maintain loans throughout their life cycle. The data fields in the system are consistent with the minimal information to maintain these loans. WIFIA Team members use information in the system consistent with intended purpose of Portfolio management of loans.

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

All internal users will be EPA employees or contractors, and required to take Information Security and Privacy Awareness Training and sign Rules of Behavior annually.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Unauthorized access jeopardizes accountability and puts the following privacy related information at risk: Names, business emails, business phone numbers, and business addresses for borrowers. 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 WIFIA Team authorizes requests for access from borrowers. Account access is setup 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 6.0 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.

To maintain business contact between the EPA team maintaining the loans and the borrowers

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.*)

A limited team of EPA \ OW users will be able to log into the application and sees a list of loans that feature the Organization/Business name and a loan number. From there, the EPA user can click on a loan and expand the record to see more detailed information. The systems primary method of retrieval uses Loan ID and Organization Name to access information.

The organization that applies for the loan will have the ability to log into a web browser and upload documents, and view documents that they have previously uploaded specific to their loan. They will not be able to view other organization's loans.

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 application resides in the general support system OIMSS in the Salesforce Gov Cloud within the Office of Chemical Safety and Pollution Prevention Org. 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:

Information may only be used for the intended purpose of the Portfolio management responsibilities previously described in the "general description/overview" section of this document. The risk to "uses of information" occurs when information is used for unintended purposes. For example, not related to management of loan closures. This jeopardizes the EPA's trust with the public and could discourage future borrowers.

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 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: