Privacy Impact Assessment (PIA) Template

FDONLINE
(Name of the Information System or Information Collection)

April 2025
Date

System/Collection Overview
FDonline is an existing, contractor operated, cloud-based system-as-a-service. It is used by members of the Ethics Office as well as other employees who are designated as financial disclosure filers by the Ethics Office. The purpose of FDonline is to provide an electronic system for FHFA employees to file required confidential financial disclosure reports and for agency ethics staff to review, certify, and store the reports.

Section 1.0 Characterization of the Information

The following questions define the scope of the information requested and/or collected as well as reasons for its collection as part of the System/Collection being procured or developed. The questions address all information collected, with emphasis on the collection of PII, such as name, address, social security number, date of birth, financial information, etc.

#	Question	Response
1.1	What information types (e.g., contact information, demographic information, employment information) are being collected, used, disseminated, or maintained in the System/Collection?	Employee business contact information; employee job position/title information; assets, income, and financial liabilities of employee, employee's spouse, and employee's dependent children; outside positions, agreements, and gifts or travel reimbursements of employee; employee spouse's employment information.
1.2	What or who are the sources of the information provided to FHFA and included in the System/Collection?	Employees who are required to file confidential financial disclosure reports enter information directly into the system.
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	For employees to file required confidential financial disclosure reports and agency ethics staff to review the reports.
1.4	How is the information provided to or otherwise obtained by the System/Collection?	Employees who are required to file confidential financial disclosure reports enter information directly into the system.

1.5	Are Social Security Numbers (SSNs) being collected or used in the System/Collection? • If yes, describe in detail: 1) The business justification for collecting or using SSNs; 2) The consequences if SSNs are not collected or used; and 3) How the SSNs will be protected while in use, in transit and in storage. • If no, state "N/A" in the response section.	N/A

Section 2.0 Uses of the Information

The following questions delineate the use of information.

#	Question	Response
2.1	How will the information be used and for what purpose?	The information will be used for agency ethics staff to review required confidential financial disclosure reports to resolve any potential conflicts of interest.
2.2	Describe any types of measures or processes in place to ensure that information is only used in the manner for which it was collected.	Only the employee submitting the confidential financial disclosure report and agency ethics staff personnel reviewing the information have access to the information. All agency ethics staff can view the reports but only the Designated Agency Ethics Official and Alternate Agency Ethics Official can provide the final certification.

Section 3.0 Retention

The following questions outline how long information will be retained after the initial collection.

#	Question	Response
3.1	How long is the information retained?	6 years
3.2	Has a retention schedule been approved by FHFA's Records Management Office and National Archives and Records Administration (NARA)? If yes, provide the corresponding General Record Schedule (GRS) or FHFA specific Records Schedule number.	GRS Schedule 2.8

Section 4.0 Notice, Access, Redress and Correction

The following questions are directed at notice to the individual, the individual's right to consent to uses of the information, the individual's right to decline to provide information, and the individual's ability to ensure the accuracy of the information collected about them.

#	Question	Response
4.1	Is the information in this System/Collection retrieved by an individual's name or personal identifier such as an SSN or other identification? • If no, please put "no" in the Response section. • If yes, the System/Collection will need to be covered by a Privacy Act System of Records Notice(s) (SORN(s)). Please provide the SORN(s) name and number or indicate that a SORN is in progress.	Yes. OGE/GOVT-2 Confidential Statements of Employment and Financial Interests
4.2	How is notice about the collection of PII provided to individuals prior to the collection for the System/Collection (e.g., direct notice, Privacy Act Statement or public notice, SORN)? If notice is not provided, explain why not.	A Privacy Act statement is provided to employees via Office of Government Ethics (OGE) Form 450 that is used to complete confidential financial disclosure reports. Employees are also informed of their requirement to submit the OGE Form 450 at the time of hire or upon assuming a position that requires filing of the OGE 450.
4.3	Is an individual's response to the request for information voluntary or mandatory?	An individual's response is mandatory.
4.4	What are the consequences if an individual declines to provide the information?	The individual may not be hired by the agency or may face disciplinary action.
4.5	What are the procedures that allow individuals to gain access to their information?	Contacting FHFA's Supervisory Ethics Program Specialist, via email at ethics@fhfa.gov.
4.6	What are the procedures for correcting inaccurate or erroneous information?	Contacting FHFA's Supervisory Ethics Program Specialist, via email at ethics@fhfa.gov.

Section 5.0 Sharing and Disclosure

The following questions define the content, scope, and authority for information sharing.

#	Question	Response
5.1	Is information shared with internal office(s) or division (s)? • If yes, please identify the FHFA office(s) or division(s) and describe the information shared and for what purpose. • If no, please state "N/A" in the response section.	N/A
5.2	Is information shared with external (outside FHFA) agencies, organizations, contractors, or other entities? For purposes of this Section, external organization(s) include Federal, state, and local government, and the private sector. • If yes, please identify the information shared, and for what purpose. • If no, skip to Section 6.	N/A
5.3	Is the sharing of PII outside the agency compatible with the stated purpose of the original information collection? • If yes and a SORN applies, identify the applicable routine uses in the SORN listed in Question 4.1. • If no and/or a SORN does not apply, identify the legal authority that permits the sharing outside FHFA.	N/A

Section 6.0 Technical Access and Security

The following questions describe technical safeguards and security measures.

#	Question	Response
6.1	Will FHFA Office of Inspector General (OIG) or non-FHFA personnel (e.g., contractor personnel, regulated entity personnel) have access to the System/Collection and information contained therein? • If yes, how will they gain access to the System/Collection? • If no, how will the agency control access to and use of that information? • Are there procedures or criteria documented in writing? If so, please describe.	No, only the employee submitting the confidential financial disclosure report and agency ethics staff personnel reviewing the information have access to the information. Access to the system is only provided by the system administrator based on a need to access the system (for filing or review). The Ethics Program maintains written internal procedures documenting when and how access is provided.
6.2	Are there any conflicts of interest with respect to the System/Collection or information? If so, identify the conflicts of interest and describe how they are addressed.	No.

6.3	Describe the type and frequency of training that is provided to users that is specifically or generally relevant to the System/Collection.	FD Online provides a customer service phone for any technical difficulties as needed. Additionally, FD Online provides webinars quarterly to discuss updates and answer questions. FHFA employees are also required to take annual ethics training and annual privacy training.
6.4	Describe the technical/administrative safeguards in place to protect the data.	FD Online is authorized under the Federal Risk and Authorization Management Program (FedRAMP). FD Online received its initial FedRAMP Authorization on August 22, 2018. It is in the continuous monitoring phase of the FedRAMP and FHFA reviews the status of ongoing assessments at least annually. FHFA has developed Customer Controls that describe the Agency's implementation of controls that are the responsibility of FHFA as the Customer Agency, and not the responsibility of the vendor. This includes the implementation of single sign-on authentication, procedures for securely managing access to the system, assigning permissions based on the concept of least privilege, and generating and reviewing audit logs.

Section 7.0 Risk

The following questions describe the risk to the information within the System or Collection.

#	Question	Response
7.1	Given the amount and type of information collected, what are the risks to an individual's privacy associated with collection of the data? Explain in detail how the loss or compromise of the information will/can affect an individual's privacy and describe how these risks are mitigated.	The loss or compromise of the employee's business information would have a minimal impact on the employee. However, information concerning an employee's income, financial assets, liabilities, outside positions, outside agreements, and gifts/travel reimbursement could lead to embarrassment and/or financial harm (e.g., targeted phishing attacks) in the event of unauthorized disclosure, especially if paired with other data outside of this system. This risk is mitigated by limiting access to the system. Access to employee confidential financial disclosure reports is limited to the submitter and a small number of agency ethics staff who review the information in the system. Further, the rigorous security standards imposed by FedRAMP reduce the risk of a breach of the system.
7.2	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	The data is retained for only 6 years, limiting the risk of inadvertent data loss or compromise by limiting the amount of data in the system. This risk is mitigated by adhering to the GRS retention schedule as well as limiting access to the system, as described above.

7.3	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	N/A