Privacy Impact Assessment (PIA) Template

FHFA TELEWORK REQUEST SYSTEM

September 2023

Tasha L. Cooper
Senior Agency Official for Privacy
(202) 649-3091
Tasha.Cooper@fhfa.gov

System/Collection Owner(s)			
Name	**E-mail**	**Division/Office**	**Office or Mobile Phone Number**
Bob Stanton	bob.stanton@fhfa.gov	OHRM	202-649-3750
Executive Sponsor			
Name	**E-mail**	**Division/Office**	**Office or Mobile Phone Number**
Monica Matthews	monica.matthews@fhfa.gov	OHRM	202-649-3374

System/Collection Overview

The FHFA Telework Request System is used to request and approve/deny telework/extended telework at FHFA. The system contains information regarding an employee's position, telework schedule, telework location and telework determination.

Employees use the system to request telework/extended telework and enter information regarding the number of telework days, telework locations, and the days of the week the employee would like to telework. Supervisors evaluate telework requests and Agency needs to determine if and how much work is suitable for telework. Supervisors then evaluate the employee's work habits, disciplinary and performance history, and personal responsibility to determine if the employee is suitable for telework and record this determination in the telework system.

Ultimately, supervisors use the information in the telework system, among other factors not contained in this system, to determine if an employee's telework request will be granted as requested, modified in part, or denied.

In addition to the employee's first line supervisor, second line supervisors make determinations for extended telework requests and may be able to see the information entered in the system by the employee.

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 name, title, supervisor, office location, division/office/branch, telework schedule, telework location(s), eligibility, and determination.
1.2	What or who are the sources of the information provided to FHFA and included in the System/Collection?	The requesting employee and their first line supervisor and if the employee requests extended telework, the second line supervisor.
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	To request telework/extended telework, to evaluate the suitability of the position and the employee for telework, to establish the telework schedule, to approve/deny telework/extended telework, and to maintain Agency records of

		telework/extended telework requests, approvals, and denials.
1.4	How is the information provided to or otherwise obtained by the System/Collection?	By the employee requesting telework and their first- and second-line supervisors.
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 to evaluate positions and people for telework/extended telework approval/denial.
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.	System access will only allow employees to access their own files, first- and second-line supervisors will only be allowed to access their own and their employees' files, and a limited number of OHRM employees will have global access to the files based on their official business need to know such information.

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?	In accordance with the Agency's retention schedule, information contained within the system is destroyed when obsolete, or superseded, or one year after employee's participation in the Telework Program ends.
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.	Yes. 2.3.040.

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. FHFA-15 and OPM/GOVT-1.
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.	The Privacy Act Notice is on the automated request form.
4.3	Is an individual's response to the request for information voluntary or mandatory?	Voluntary.
4.4	What are the consequences if an individual declines to provide the information?	Employees that do not provide the required information may not be allowed to telework. Supervisors are required to respond to requests for telework or be subject to discipline if no response is provided to a requesting employee.
4.5	What are the procedures that allow individuals to gain access to their information?	The system will be available to employees, supervisors, and managers with appropriate access upon login to FHFA's Network. These individuals can access their information in accordance with the System of Records Notice.
4.6	What are the procedures for correcting inaccurate or erroneous information?	OTIM can access the system and correct inaccurate information. When an employee's supervisor changes in FHFA's Active Directory, the telework system updates to allow only the new supervisor to view the employee's information. Employees are also able to have inaccurate information corrected in accordance with the System of Records Notice.

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.	Managers and supervisors of employees who request telework and OHRM will have access to the information in the system to approve or deny telework requests and manage the telework program.
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.	No. Personal information is not shared with external organizations; however, data is collected in the aggregate to respond to OPM reporting requirements.
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 a 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.	Generally, non-FHFA personnel will not have access to the System and information contained therein because telework is limited to Federal Employees only. OTIM Admins, however, may include contractors who have access to the system but not the data contain therein as information contained within the system is encrypted.
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.	All FHFA employees are required to undergo Security, Privacy, and Records and Information Management (RIM) training at new employee onboarding training and annually thereafter. In addition, all FHFA users with elevated privileges receive specialized security training, and role-based privacy awareness training for those individuals whose work duties and responsibilities involve the collection, use, storage, access, or maintenance of PII.
6.4	Describe the technical/administrative safeguards in place to protect the data.	As documented in the System Security and Privacy Plan (SSPP), access to FHFA Telework Request System is limited to those with a business need to access and who have been approved for access by the system owner. Role-based access controls are designed into the system and users are granted the least privileged role required to carry out their responsibilities. FHFA Telework Request System is hosted by FHFA and accessible only to FHFA users with valid Active Directory accounts. Technical and administrative safeguards are documented within the SSPP and tested prior to authorization and annually thereafter as part of FHFA's assessment and authorization (A&A) process and consistent with the NIST Risk Management Framework. These safeguards include, but are not limited to procedures for securely managing access to the system, assigning permissions based on the concept of least privilege, generating, and reviewing audit logs, data encryption, etc.

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.	If a user's data is exposed, they could be subjected to unauthorized or accidental disclosure of their personal address. To prevent unauthorized use of the data, access to the data is limited to those with an official need-to-know and who have signed and are subject to the FHFA System Rules of Behavior and User Acknowledgment.
7.2	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	There are minimal risks associated with the length of time the data is retained. The data is maintained for the length of time that the employee is employed within OHRM and is in accordance with the GRS. Access to this data is

		controlled and only provided as needed as described in this document.
7.3	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	N/A. Information is not shared externally.