Privacy Impact Assessment (PIA)

WORKFLOW TRACKING SYSTEM (WTS)
(Name of the Information System or Information Collection)

April 2026
Date

System/Collection Overview
The Workflow Tracking System (WTS) was created to provide a central workflow path for the Office of Single and Multifamily Policy (OSMP) to facilitate submission review, analysis, escalation, sign-off, closeout and monitoring of policy items and correspondence. WTS is a web-based, stand-alone application on the FHFA Intranet that allows for both data entry and automated data import of information from the Agency's Status Tracking and Report System (STAR), eliminating manual processes, single person dependencies, and SharePoint for manual issue tracking. WTS enables efficient business processes (i.e., integrated systems and paper-free reviews through closeout) and decision making within the Division of Housing Mission and Goals (DHMG). The tool allows Policy Analysts to drive review processes, has appropriate checkpoints and concurrence points, contains advanced reporting capabilities, and enhances collaboration, recordkeeping, and traceability across DHMG.

Section 1.0 Characterization of the Information

The following questions address the scope of the personally identifiable information (PII) requested and/or collected. PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. PII includes, but is not limited to, name, address, Social Security number, date of birth, financial information, and demographic information.

#	Question and Response
1.1	***What and whose PII is being collected, used, disseminated, or maintained?***
	The names and contact information of FHFA employees and contractors are collected, as well as the names, titles, and business contact information of third parties such as employees from agencies outside of FHFA or employees of Fannie Mae or Freddie Mac.
1.2	***If Social Security Numbers (SSNs) are included, describe in detail:*** ***1) The business justification for collecting or using SSNs;*** ***2) The consequences if SSNs are not collected or used;*** ***3) How the SSNs will be protected while in use, in transit and in storage.***

	Not applicable.
1.3	***How is the PII obtained? If individuals are not providing their own PII directly, describe where the information originates and any intermediaries it goes through before being provided to FHFA. Include a description of the mechanism by which the PII is provided to/obtained by FHFA.***
	For internal FHFA users, PII is obtained via Microsoft Active Directory, a centralized directory service used for authentication. For external parties, analysts manually enter PII into the system. This information could come from the analysts' own knowledge, emails from external parties, public reports from Fannie Mae/Freddie Mac, or analysts' meeting notes. Through the STAR system, the Fannie Mae/Freddie Mac will also send documents to the system that may include the name, email, and phone number of external parties. When these documents are sent, WTS automatically updates system information based on any information received from STAR. No information is collected directly from the individual. WTS also receives information regarding correspondence from members from FHFA's Correspondence Tracking System (CTS), including the name of the sender. This information can be submitted manually by WTS users or directly from CTS.
1.4	***How will the PII be used and for what purpose?***
	The information will be used to provide a central workflow path for OSMP submission review, analysis, escalation, sign-off, closeout, and monitoring of policy issues. PII specifically is used to identify points of contact for projects and to track milestones and tasks within them.
1.5	***Is there a risk that PII other than that described above will be collected? If no, explain why not. If yes, explain the risk and how the risk is mitigated.***
	The system contains free text fields that creates a risk that analysts may enter additional PII other than individuals' names, job titles or business contact information. To mitigate this risk, a user guide is provided to system users that instructs them to only include PII in the system when necessary.

1.6	***Is there a risk that the PII collected will be inaccurate? If no, explain why not. If yes, explain the risk and how the risk is mitigated.***
	There is a risk that the PII collected will be inaccurate since the information could come from less reliable sources such as user's own knowledge or an analyst's meeting notes. Manual entry also introduces the risk of typographical errors. To address this risk, any outdated or incorrect information, once discovered, can be updated within the system by the analyst who is assigned the entry. The only way for incorrect or outdated information to be discovered would be for system users to review the entries.

Section 2.0 General

The following questions address general information about the information in the system, including how the information will be used and for what purpose.

#	Question and Response
2.1	***What is the legal authority for the collection?***
	The legal authority for the collection is 12 U.S.C. § 4513(a).
2.2	***Is the collection of information subject to the Paperwork Reduction Act? If yes, what is the OMB Control Number for the collection?***
	Entries in the system are not created in response to requests from FHFA for specific information, therefore the Paperwork Reduction Act does not apply.
2.3	***Is this a new PIA or an update to an existing PIA?***
	This is a new PIA.
2.4	***Is the system internally operated or operated by a third-party (e.g., contractor)? If not internally operated, please identify the third party.***

	This system is internally operated.
2.5	***How is the risk of improper use of the PII by FHFA employees/contractors mitigated? If PII is shared with third parties, how will the risk of improper use by those parties be mitigated?***
	The risk of improper use of PII by FHFA employees/contractors is mitigated by providing a user guide to system users that explains the procedures for entering PII, including the best practice of minimizing the use of PII within the notes section of the system and encouraging users to only input necessary information. It is also mitigated by FHFA employees/contractors receiving annual privacy and information security training, which ensures they remain aware of the risks and consequences of improper use of PII. PII included in WTS is not shared with third parties.

Section 3.0 Retention

The following questions address how long PII will be retained after the initial collection.

#	Question and Response
3.1	***How long is the PII retained?***
	The items in the system are subject to a 30-year retention period.
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.***
	The retention period is subject to Comprehensive Records Schedule (CRS) 2.3b.

Section 4.0 Notice, Individual Access, and Correction

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

#	Question and Response
4.1	***Is information about an individual retrieved by an individual's name or personal identifier such as name, email address, or date of birth? If yes, identify the applicable System of Record Notice (SORN).***
	Information about an individual is not retrieved by an individual's name or personal identifier.
4.2	***How is notice about the collection of PII provided to an individual prior to collection from that individual? If notice is not provided, explain why.***
	Not applicable. Information is not collected directly from individuals and the WTS is not a "system of records" under the Privacy Act and therefore notice of the collection of PII is not required.
4.3	***Is an individual's response to the request for PII voluntary or mandatory?***
	Not applicable as information is not collected directly from individuals.
4.4	***What are the consequences if an individual declines to provide the requested PII?***
	This is not applicable. The PII in the system is not provided directly by the individual for the purposes of this system.

4.5	***What are the procedures that allow individuals to gain access to their PII?***
	This is not applicable as this system and the records and information therein are not subject to the Privacy Act.
4.6	***What are the procedures for individuals to correct or update information about them?***
	This is not applicable as this system and the records and information therein are not subject to the Privacy Act.

Section 5.0 Sharing and Disclosure

The following questions address the content, scope, and authority for sharing PII.

#	Question and Response
5.1	***Is PII shared with other offices or divisions within FHFA? If yes, identify the other offices/divisions and describe the purpose of or business need for sharing the PII.***
	PII from the system is not shared with divisions or offices other than those within DHMG. Staff from the Office of the Chief Information Officer may also have access to PII in the system as part of their system maintenance responsibilities.
5.2	***Is PII shared with individuals or entities outside of FHFA? External entities include other Federal agencies, state or local governments, regulated entities, FHFA-OIG, and Congress. External entities do not include FHFA contractors that receive PII as needed in their performance of work for FHFA.*** ***If yes, please identify the PII shared, and for what purpose or business need.***

	No information is shared outside of FHFA.
5.3	***If PII is shared with external entities, describe how the information sharing is compatible with the purpose for which the PII was collected.*** • ***If a SORN applies, identify the applicable routine uses in the SORN listed in Section 4.1.*** • ***If a SORN does not apply, describe 1) whether notice of the PII sharing was provided and if so, how; and 2) how the sharing of PII is consistent with the purpose for which the information was collected. Sharing with Congress, FHFA-OIG or the Government Accountability Office pursuant to the statutory authorities of those entities need not be addressed.***
	Not applicable.
5.4	***Describe how the risk of intentional or inadvertent disclosure of PII by FHFA employees/contractors is mitigated. (Address both disclosures within FHFA and disclosures to external parties.)***
	The risk of disclosure of PII by FHFA employees is mitigated by annual privacy training given to all FHFA employees and contractors including system users.
5.5	***If PII will be shared with external parties, describe how the risk of improper disclosure of the information by individuals or entities outside of FHFA is mitigated.***

	Information will not be shared with external parties.

Section 6.0 Technical Access and Security

The following questions address technical safeguards and security measures.

#	Question and Response
6.1	***Will individuals other than FHFA employees and FHFA contractor personnel performing official FHFA duties have access to the system containing the PII? If yes, how will access to the system be granted and controlled with respect to these external parties?***
	No individuals other than FHFA employees and contractor personnel have access to the system.
6.2	***Is any system-specific training or guidance related to PII or privacy provided to users of the system? If so, please describe.***
	A user guide is provided to every system user that encourages users to minimize the PII entered into the system to that which is necessary.
6.3	***Describe the technical/administrative safeguards in place to protect the PII.***
	Access is limited to users with an FHFA device. Further, only users who require access for business purposes and have received approval from the system owner are permitted to use the system. FHFA users are granted access based upon FHFA Active Directory roles. Role-based access and least privilege ensure users are granted necessary access and data is protected. The system owner receives and is responsible for reviewing monthly audit logs in accordance with the system security and privacy plan. The system uses standard data encryption protocols to protect data at rest and while in transit.