



Privacy Impact Assessment (PIA)

REASONABLE ACCOMMODATIONS AND PERSONAL ASSISTANCE
SERVICES INFORMATION SYSTEM
(Name of the Information System or Information Collection)

March 2026
Date

System/Collection Overview

The Reasonable Accommodations and Personal Assistance Services Information System is an existing FHFA-operated system used to document the processing of requests for reasonable accommodations, religious accommodations, and personal assistance services for qualified FHFA employees and job applicants, excluding Office of Inspector General (OIG) employees and job applicants. The purpose of the system is to allow FHFA to collect and maintain all records related to requests for reasonable accommodations, religious accommodations, and personal assistance services. The system also allows FHFA to track all actions, recommendations, and decisions throughout the process, as well as report aggregated data to the appropriate entities to ensure compliance with applicable laws and regulations.

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	<p><i>What and whose PII is being collected, used, disseminated, or maintained?</i></p> <p>An individual's name, contact information, position, type of accommodation requested/granted (e.g., desk, keyboard), personal assistance requested/granted (e.g., retrieving out of reach material, travel assistance), and/or religious accommodation requested/granted (e.g., adjusted work hours/break times, leave for religious observances) is maintained in the system. Additionally, an employee's religion and medical information, such as their limitations, duration of medical condition, etc., may also be maintained in the system. Covered individuals include employees, former employees, and applicants for employment.</p>
1.2	<p><i>If Social Security Numbers (SSNs) are included, describe in detail:</i></p> <ol style="list-style-type: none"><i>1) The business justification for collecting or using SSNs;</i><i>2) The consequences if SSNs are not collected or used;</i><i>3) How the SSNs will be protected while in use, in transit and in storage.</i>

	<p>SSNs are not maintained in the system. SSNs (full, truncated, or redacted) may be captured in documents that are provided to the Reasonable Accommodation Coordinator, but that information is not entered or uploaded into the system. The documents that are provided to the coordinator are stored in the Agency's electronic file system.</p>
1.3	<p><i>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.</i></p> <p>The sources of the information provided include employees or applicants requesting an accommodation and/or assistance, their family members or authorized representatives, and FHFA management officials. As part of the request process, these individuals provide their names and other relevant information. The information is entered electronically into FHFA forms and then manually entered into the system by the Reasonable Accommodation Coordinator or their representative.</p>
1.4	<p><i>How will the PII be used and for what purpose?</i></p> <p>The purpose of the collection is to document requests for reasonable accommodations, religious accommodations, and personal assistance services. It is used to track and report all actions, recommendations, and decisions. Additionally, the information is used to facilitate the processing of these requests and meet recordkeeping and reporting requirements related to this process.</p>
1.5	<p><i>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.</i></p> <p>No. While individuals can provide more information than is necessary for their request, that information would not be entered into the system. It would be contained in another system with appropriate protections.</p>
1.6	<p><i>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.</i></p>

	The risk of collecting inaccurate PII is minimal. Because information may come from sources other than the individual, such as family members, authorized representatives, or FHFA management officials, there is some potential for errors. The risk is mitigated by restricting input to authorized individuals and allowing the person whose PII is collected an opportunity to review and confirm all information provided.
--	---

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	<p><i>What is the legal authority for the collection?</i></p> <p>The Rehabilitation Act of 1973 (29 U.S.C. 791); 29 CFR part 1630; Executive Orders 13163, 13164 and 13548; Equal Employment Opportunity Commission (EEOC) Policy Guidance on Executive Order 13164; EEOC Enforcement Guidance: Application of the Americans with Disabilities Act (ADA) to Contingent Workers Placed by Temporary Agencies and Other Staffing Firms; Title VII of the Civil Rights Act of 1964 (42 U.S.C. 2000e); and 29 CFR part 1605.</p>
2.2	<p><i>Is the collection of information subject to the Paperwork Reduction Act? If yes, what is the OMB Control Number for the collection?</i></p> <p>No. Information in this system is not collected in a manner that is subject to the Paperwork Reduction Act.</p>
2.3	<p><i>Is this a new PIA or an update to an existing PIA?</i></p> <p>This is an update to an existing PIA.</p>
2.4	<p><i>Is the system internally operated or operated by a third-party (e.g., contractor)? If not internally operated, please identify the third party.</i></p>

	The system is internally developed and operated by FHFA.
2.5	<p><i>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?</i></p> <p>Access is only granted to Office of Human Resource Management (OHRM) employees and/or contractors involved in processing requests. For information shared with the EEOC, the privacy risk to the individual is minimal. The information is aggregated and all PII is removed before sharing it with external entities. FHFA's IT Security Branch has established procedures for securely managing access to the system and for reviewing user activity for indications of inappropriate use.</p>

Section 3.0 Retention

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

#	Question and Response
3.1	<p><i>How long is the PII retained?</i></p> <p>Information is retained for 3 years from the cut-off date, which is the date of the employee's separation from FHFA or the conclusion of any related appeal, whichever is later.</p>
3.2	<p><i>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.</i></p> <p>Yes. GRS 2.3.020.</p>

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	<p><i>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).</i></p>

	Yes. FHFA-18, Reasonable Accommodation and Personal Assistance Services Information System is the applicable SORN.
4.2	<p><i>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.</i></p> <p>A Privacy Act Statement describing FHFA’s purpose for collecting the information, the authority for the collection, how the information will be used, and the consequences of not providing it is at the bottom of the relevant forms that are used for the collection. Direct notice is provided to employees if they are not provided with a form. Notice is also provided via the above-referenced SORN.</p>
4.3	<p><i>Is an individual’s response to the request for PII voluntary or mandatory?</i></p> <p>The response to the request for information is voluntary.</p>
4.4	<p><i>What are the consequences if an individual declines to provide the requested PII?</i></p> <p>An individual may not be considered for an accommodation or service if the requested information is not provided.</p>
4.5	<p><i>What are the procedures that allow individuals to gain access to their PII?</i></p> <p>Individuals can gain access to their information by contacting FHFA’s Privacy Office as set forth in the SORN, FHFA-18 and FHFA’s Privacy Act Regulations, 12 CFR 1204. More information is available at FHFA’s Privacy webpage: Privacy FHFA.</p>
4.6	<p><i>What are the procedures for individuals to correct or update information about them?</i></p>

	Inaccurate or erroneous information can be corrected by contacting FHFA’s Reasonable Accommodation Coordinator or the Privacy Office as set forth in the SORN, FHFA-18 and FHFA’s Privacy Act Regulations, 12 CFR 1204. More information is available at FHFA’s Privacy webpage: Privacy FHFA .
--	---

Section 5.0 Sharing and Disclosure

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

#	Question and Response
5.1	<p><i>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.</i></p> <p>Yes. The information collected may be shared with other OHRM offices if necessary to perform human resources functions. Information may also be provided to FHFA’s Equal Employment Opportunity (EEO) Office if required to perform EEO-related functions and to the Office of General Counsel if legal guidance is needed when processing a request. The Office of Facilities Operations Management and the Office of Chief Information Officer may review non-routine accommodation requests related to their assigned functions to assess the feasibility and reasonableness of an accommodation prior to a decision to grant or deny such accommodation.</p>
5.2	<p><i>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.</i></p> <p>Information from the system may be shared with the EEOC, the Merit Systems Protection Board, or a federal court if the information is relevant to litigation in those forums. The information may also be made available to attorneys, including those at the Department of Justice (DOJ), providing representation in those forums.</p> <p>Aggregated, non-identifiable information is shared with the EEOC, in accordance with Management Directive 715 (MD-715). The reasonable accommodation and personal assistance services information provided to EEOC is aggregated (e.g., number of employees of a particular sex or race) and therefore does not contain PII. That information is provided to assist EEOC with guidance and oversight of the program, including determinations of any deficiencies in the agency’s EEO program. Information may also be shared with other third parties who are legally required to access the information for business-related purposes.</p>

5.3	<p><i>If PII is shared with external entities, describe how the information sharing is compatible with the purpose for which the PII was collected.</i></p> <ul style="list-style-type: none"> <i>If a SORN applies, identify the applicable routine uses in the SORN listed in Section 4.1.</i> <i>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.</i>
	<p>FHFA may share certain information permitted by the routine uses listed in SORN, FHFA-18. In particular, routine use 15 permits the sharing of PII from the system with DOJ, (including United States Attorney Offices), or other Federal agencies conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is necessary to the litigation and FHFA or an employee of FHFA are a party to the litigation. In addition, FHFA is required to report aggregated information to the EEOC, as noted in routine use 11, and in accordance with MD-715 referenced in section 5.2 above.</p>
5.4	<p><i>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.)</i></p>
	<p>The risk of improper disclosure of PII is mitigated by granting access only to individuals who are responsible for processing the requests and/or making decisions related to the requests. The risk is further mitigated by requiring mandatory privacy training for all agency employees and contractors, which includes breach response protocols, and role-based training for those who are granted access to the system. Additionally, because the system is developed and hosted internally by FHFA, the risk of data loss due to hacking or other malicious activity is further reduced through the technical, administrative, and physical safeguards noted in section 6.3.</p>
5.5	<p><i>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.</i></p>
	<p>For information shared in litigation, the risk of improper disclosure is generally low as these forums have established processes, including imposing protective orders, for protecting sensitive information.</p> <p>For information shared with the EEOC for data reporting purposes, the privacy risk to the individual is minimal. The information is aggregated and all PII is removed before sharing it with external entities.</p>

Section 6.0 Technical Access and Security

The following questions address technical safeguards and security measures.

#	Question and Response
---	-----------------------

6.1	<p><i>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?</i></p>
	<p>Yes. OIG may be granted access by the system owner if necessary for OIG-related work. Otherwise, only those involved in processing/decision making are granted access to the system by the system owner. Individual access permissions are reviewed and certified annually. Access control procedures are documented in the General Support System (GSS) System Security and Privacy Plan (SSPP), and the enterprise Access Control Standard.</p>
6.2	<p><i>Is any system-specific training or guidance related to PII or privacy provided to users of the system? If so, please describe.</i></p>
	<p>No system-specific training is provided to the users of the system. However, system users are required to take annual role-based privacy training related to the collection and protection of PII.</p>
6.3	<p><i>Describe the technical/administrative safeguards in place to protect the PII.</i></p>
	<p>The system is stored on the FHFA GSS and protected by the safeguards described in the FHFA GSS SSPP and the GSS PIA. These safeguards include, but are not limited to, role-based access controls that restrict access to information based on Active Directory groups and permissions, auditing of files access and modification, data encryption. The GSS is integrated with the enterprise continuous monitoring strategy in alignment with the Risk Management Framework.</p>