Privacy Impact Assessment (PIA)

USAi
(Name of the Information System or Information Collection)

March 2026
Date

System/Collection Overview
USA Intelligence (USAi) is a secure, multi-tenant generative artificial intelligence (GenAI) platform/service administered by the General Services Administration (GSA). USAi operates in a FedRAMP-authorized cloud environment, approved at the moderate impact level. USAi provides federal agencies with access to select GenAI large language models offered by commercial providers. FHFA has a memorandum of understanding (MOU) with GSA to test and evaluate those models. FHFA anticipates testing several use cases with one or more USAi GenAI models. The use cases will include uploading, storing, and processing information that includes personally identifiable information (PII) within the USAi environment.

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 USAi system will be used by FHFA employees and contractors. To access the system, users must sign-in using their FHFA credentials and authenticate using FHFA's single sign-on (SSO) system. FHFA's SSO system provides the following PII to the USAi system: user first and last name, user email address, and user ID (in the form of the user's logon name). The system captures login/activity records and tracking data (cookies, geolocator, IP address, etc.). USAi collects the following interaction information: user prompts and responses; document content, text formatting, and basic metadata (i.e., file type, file name, and word count) from uploaded documents; search queries generated by the GenAI chat model as a result of prompts; user ratings (i.e., thumbs up or down ratings) and user feedback; device/browser data including Internet Protocol address, location, the language the user is browsing in, and the operating system and browser used; dates and times of access, the actions taken by users, and information about user interactions, such as where the user navigates, what the user clicks, and Application Programming Interfaces (APIs) requested by the user. More information is available in the USAi Privacy Policy available here: Privacy Policy | USAi.

	In addition to the user PII necessary to access and use the system, individual FHFA use cases will also upload and process PII. The individual use cases and the PII specific to those use cases are described separately in the relevant sections of this PIA. **Use Cases** **Comments Project**: This use case relies on comments submitted during the request for proposal or input process that is related to rulemaking and other regulatory activities. PII may include a commenter's first and last name, location information (city and state only), email address, and the organization the commenter is affiliated with. Information also includes any PII that individuals may have included in their comments. The PII submitted by commenters is generally made publicly available as individual comments and the associated commenter information are posted to FHFA's public website. Individuals submitting comments are notified of the fact that their PII will be made publicly available in the notice soliciting public comments. **Engineering Reports**: This use case processes engineering reports that inspect or assess property conditions of residential properties. PII may include information from an engineer (e.g., first and last name, business location, and professional contact information) as well as a residential property (street address, homeowner or condo association names, and visual and textual documentation of the property's physical condition). The PII submitted is part of a due diligence business practice for a property to receive approval to proceed with mortgage underwriting processes. Individuals voluntarily have their properties go through this process in order to assess eligibility for mortgage funding from Fannie Mae or Freddie Mac. **Suspended Counterparty Program**: This use case relies on case materials maintained by FHFA's Office of General Counsel as part of the Suspended Counterparty Program (SCP), which evaluates referrals involving potential misconduct related to mortgage transactions. PII may include an individual's first and last name, contact information (such as residential or business address, email address, and telephone number), organizational affiliation, and information contained within legal, investigative, or supporting documentation. The PII included in SCP case files is collected as part of FHFA's statutory responsibilities and is already maintained within FHFA's existing internal systems. If an individual is suspended by FHFA under the SCP, a final suspension order is made public. Final suspension orders may include an individual's name, city and state of residency, and other information relevant to the individual's suspension, including business transactions and information regarding criminal convictions and administrative sanctions imposed by other federal agencies.
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.*** **Use Cases** **Comments Project**: SSNs are not requested as part of the comment process and commenters should not provide such information. **Engineering Reports**: SSNs are not included in the reports and will not be uploaded to USAi. **Suspended Counterparty Program**: SSNs will not be uploaded to USAi.

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.***
	PII for system access is obtained via FHFA's SSO system. **Use Cases** **Comments Project**: Information is uploaded by FHFA staff from existing data sources. PII is originally provided to FHFA directly by commenters when submitting their comments. **Engineering Reports**: Information is uploaded by FHFA staff from existing data sources. PII is originally provided to FHFA by Fannie Mae or Freddie Mac from engineers who have submitted their professional reports. **Suspended Counterparty Program:** Information is uploaded by FHFA staff from referrals provided to FHFA by its regulated entities, the FHFA Office of Inspector General (OIG), or other federal agencies. Information is also gathered through established SCP processes.
1.4	***How will the PII be used and for what purpose?***
	System user PII is used by GSA to: 1) provide, maintain, and secure the service; 2) authenticate users; 3) enforce usage rate limits; 4) monitor for, prevent, and respond to security incidents or prohibited uses; 5) assist users with support and troubleshooting. FHFA may use system user PII and system interaction information to assess the use of the system and monitor for appropriate use. **Comments Project**: Information is collected to analyze and respond to comments received by FHFA on proposed rulemakings and requests for information. **Engineering Reports**: Information is collected to analyze professional reports for the quality of reported information and suggest potential improvements to data collection and inspection. **Suspended Counterparty Program**: Information is used to evaluate referrals involving potential misconduct related to mortgage transactions and to support FHFA's determination of whether an individual or institution should be suspended from doing business with FHFA's regulated entities. Specifically, USAi will be used to review and summarize existing SCP case materials, identify relevant facts and timelines, assist in preparing draft requests for information and proposed or final suspension packages, and support internal analysis and documentation.

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.***
	For system user PII, the risk of collecting PII other than that described above is extremely low as the SSO system automates provision of PII necessary for user access. **Use Cases** **Comments Project**: No. The use of GenAI models within USAi does not involve a new information collection. The information has already been collected via the notice/comment process. **Engineering Reports**: No. The use of GenAI models within USAi does not involve a new information collection. The information has already been collected via the property inspection process. **Suspended Counterparty Program**: No additional PII is collected. USAi does not introduce new information collections, and SCP staff upload only documents already held by FHFA.
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.***
	With respect to system user PII, the risk of collecting inaccurate PII is extremely low. FHFA's SSO system provides verified user information. **Use Cases** **Comments Project**: The use of USAi does not introduce any new risks that the PII will be inaccurate as it is being uploaded from an existing data source. The risk of inaccurate PII from the original collection is relatively low as the information was obtained directly from individuals who had the option to submit the information anonymously, which would reduce the incentive to provide inaccurate information. Further, although information such as email address, city/state, and organization may become outdated over time, it is presumably accurate at the time of submission. Moreover, the anticipated analysis of comments received does not require the PII to be up to date. **Engineering Reports**: The use of USAi does not introduce any new risks that the PII will be inaccurate as it is being uploaded from an existing data source. The risk of inaccurate PII from the original collection is relatively low as the information was obtained directly from professional reports. The anticipated analysis of reports received does not require the PII to be up to date. **Suspended Counterparty Program**: The use of USAi does not introduce new risks that the PII will be inaccurate as it is uploaded from an existing data source. All PII originates from SCP materials already collected and maintained by FHFA. Any inaccuracy would stem from the source document, not the AI tool.

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?***
	For system user PII, 12 U.S.C. § 4513(a)(2)(B). **Comments Project**: 12 U.S.C. § 4526. **Engineering Reports**: 12 U.S.C. § 4513b and 12 U.S.C. § 4514. **Suspended Counterparty Program**: 12 U.S.C. § 4513(a)(2) and (b)(2)(B)(iii), and 12 U.S.C. § 4526(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?***
	No. The use of USAi will not require a new information collection as the use cases rely on information already collected. PRA procedures were followed where applicable.
2.3	***Is this a new PIA or an update to an existing PIA?***
	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.***
	The system is externally operated by GSA.
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?***

	Access to system user PII and PII for each use case is limited to employees and contractors within FHFA with a business need to access the information. FHFA staff working on a particular use case do not have access to information in USAi for other use cases unless they also have a business need to access that information. FHFA employees and contractors receive annual privacy and information technology (IT) security training regarding the proper use of PII and must agree to and sign annually IT security rules of behavior, which reiterate the adverse consequences that may result from improper use of PII.

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?***
	Within 30 days of the conclusion of the MOU with GSA or no later than July 2026, GSA will delete all FHFA raw usage logs, delete user accounts created, and coordinate with GSA's IT Security office to cleanse or otherwise sanitize FHFA data from the platform. Work products that are generated using USAi are exported to FHFA's network and retained in accordance with the applicable records retention schedule, which will vary depending on the record.
G3.2	***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 5.2, Item 010 (Transitory Records)

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).***
	For system user information, FHFA and GSA do not search the USAi platform by personal identifier. **Use Cases** **Comments Project**: No. **Engineering Reports**: No. **Suspended Counterparty Program**: No
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. The use of USAi does not require a new information collection. Where applicable, notice was provided to users at the time of the original information collection.
4.3	***Is an individual's response to the request for PII voluntary or mandatory?***
	Not applicable as the use of USAi does not require a new information collection.
4.4	***What are the consequences if an individual declines to provide the requested PII?***

	Not applicable.
4.5	***What are the procedures that allow individuals to gain access to their PII?***
	To the extent information is derived from an underlying system of records that is subject to the Privacy Act, individuals may make a Privacy Act records request as described on FHFA's Privacy website: https://www.fhfa.gov/about/privacy.
4.6	***What are the procedures for individuals to correct or update information about them?***
	To the extent information is derived from an underlying system of records that is subject to the Privacy Act, individuals may make a records amendment request under the Privacy Act as described on FHFA's Privacy website: https://www.fhfa.gov/about/privacy.

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.***
	User activity data may be shared within FHFA with individuals in any FHFA office/division who have a need to know the information. Information may be shared to evaluate the GenAI models used and to ensure appropriate user activity. **Use Cases** **Comments Project**: The PII of commenters may be shared with other offices or divisions within FHFA for the purpose of evaluating and responding to comments received as well as evaluating the performance of the GenAI model. As described in section 1.1, the commenters' PII is generally made publicly available as part of the notice and comment process. **Engineering Reports**: The PII may be shared with other offices or divisions within FHFA for the purpose of evaluating the written reports and evaluating the performance of the GenAI model.

	Suspended Counterparty Program: The PII may be shared with other offices or divisions within FHFA for the purpose of evaluating the GenAI-created documents and the performance of the GenAI model.
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.***
	GSA staff have access to a user's name, work email address, and user ID for the purpose of operating the system. Although the underlying GenAI models are provided by commercial vendors, those vendors do not have access to user prompts, model responses, or documents uploaded to the system. **Use Cases** **Comments Project**: As described in section 1.1, the commenters' PII is generally made publicly available as part of the notice and comment process. However, this sharing is unrelated to the use of USAi. **Engineering Reports**: No. **Suspended Counterparty Program**: As described in Section 1.1, some PII is made public in final suspension orders. Information may also be shared with the FHFA-OIG where relevant to an FHFA-OIG audit or investigation. However, this sharing is unrelated to the use of USAi. Otherwise, PII is not shared with external entities.
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.***
	The PII for system users that is shared with GSA is limited to name, work email address, and user ID. Employees and contractors impliedly consent to the use of such information as part of their employment or contract with the agency. Further, employees and contractors are notified upon logging onto federal IT systems that their activity may be monitored and they have no expectation of privacy with regard to using such systems. Additionally, FHFA-19, Computer Systems Activity and Access Records System permits the sharing of system user PII with contractor personnel and others performing work on a contract or project for FHFA. **Comments Project**: FHFA-22, Online Forms, permits the sharing of PII received with contractor personnel and others performing work on a contract or project for FHFA. Further, one of the stated purposes of FHFA-22 is to respond to and make public comments received. A Privacy Act notice is provided at the time of submission. **Engineering Reports**: Not applicable. **Suspended Counterparty Program**: FHFA-23, Suspended Counterparty Program, permits the sharing

	of PII received with contractor personnel and others performing work on a contract, service, cooperative agreement, or project for FHFA. FHFA-23 also permits the sharing of records with federal agencies charged with responsibility for investigating violations or potential violations of law as well as to federal agencies for the purpose of performing audit or oversight operations as authorized by law.
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.)***
	Access is restricted to authorized personnel ensuring employees and contractors access only the minimum data necessary for their duties. The risk of improper disclosure is further mitigated by providing training to FHFA employees/contractors with respect to protecting PII. Documents are also marked as Controlled Unclassified Information, where appropriate.
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.***
	Access by GSA personnel is limited to instances where it is required to perform official duties. GSA personnel receive mandatory IT security and privacy training.

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?***
	Access by GSA personnel is limited in accordance with appropriate security protocols to those individuals who require access to perform official duties. Although the underlying GenAI models are provided by commercial vendors, those vendors do not have access to user prompts, model responses, or documents uploaded 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.***
	No.
6.3	***Describe the technical/administrative safeguards in place to protect the PII.***
	USAi employs encryption of data in transit using TLS 1.2+, and at-rest using AES-256 encryption enforced via AWS Key management store on all S3 buckets, databases, documentdb clusters, and the underlying volumes for all elastic kubernetes storage nodes. This ensures that all application data, logs, and authenticators stored by the system are encrypted. USAi also uses AWS secrets manager to store, rotate, and retrieve all sensitive credentials, such as db passwords and 3rd party API keys.