



Privacy Impact Assessment

FHFA-OIG Case Management System (CMS)
(SYSTEM NAME)

July 7, 2025

DATE

Overview

This section provides an overview of the System and addresses the following:

- The System name and the division/office that owns the System;
- The purpose of the program, System, or technology and how it relates to the agency's mission; and
- A general description of the information in the System.

Date submitted for review: July 7, 2025

System Owner(s)			
Name	E-mail	Division/Office	Office Phone Number
Kimberly P. Davis	Kimberly.Davis@fhfaoig.gov	Office of Investigations	(202) 730-4913
System Overview: Briefly describe the purpose of the program, System, or technology, and the information in the System, and how it relates to FHFA-OIG's mission.			
<p>In conducting investigations, FHFA-OIG employees are required to record all investigation activity and document all information in case files. The Case Management System (CMS) is the Office of Investigations' central system for holding case file records and managing investigative resources. The CMS includes documentation from case inception to case closure. FHFA-OIG has prepared this revised Privacy Impact Assessment (PIA) to summarize the privacy risks and risk mitigation actions arising through the establishment of an Investigative Index File within CMS.</p> <p>The CMS provides management for cases, records, tasks, workflow, and collected items, as well as search and reporting capabilities. The CMS provides FHFA-OIG employees with the ability to create case documents and submit them through an electronic workflow process. Supervisors and others involved in the approval process can review, comment, and approve the insertion of documents into the appropriate electronic case files. Upon approval, the user uploads the documents into CMS, and they become part of the official FHFA-OIG case file. The CMS maintains an auditable record of all transactions. It also provides web-based access for all authorized users and a search and indexing capability, allowing access to all relevant data for which the user has permission.</p> <p>The CMS is used to maintain the following types of information: (1) complaints received by FHFA-OIG, including those from individuals and their representatives, oversight committees, and others who conduct business with FHFA-OIG; (2) information relevant to efforts to resolve those complaints; (3) information collected as part of investigations conducted by FHFA-OIG's Office of Investigations; and (4) correspondence specific to investigations received by FHFA-OIG from individuals and their representatives, oversight committees, and others who conduct business with FHFA-OIG, and the responses thereto.</p>			

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 program, System, or technology being developed. The questions address all information collected, with more emphasis provided on the collection of PII, such as name, address, social security number, date of birth, financial information, etc.

No.	Question	Response
1.1	What information is being collected, used, disseminated, or maintained in the System?	The CMS contains personally identifiable information (PII) of complainants, investigatory targets, witnesses, and other persons contacted as part of an investigation. Collected PII may include name, address, social security number, photograph, and date of birth, as well as financial information such as loan amounts, lender data, mortgage qualification information, and other relevant financial data.
1.2	What or who are the sources of the information in the System?	Information in the CMS is collected from complainants, the general public, law enforcement partners, Congressional members/staff, FHFA employees, or employees of FHFA-regulated entities and other financial institutions. Other information is obtained from persons, entities, and agencies contacted by FHFA-OIG as part of an investigation.
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	The purpose of collecting the information is to build and conduct criminal, civil, and administrative investigations against individuals and entities for potential violations of federal laws or regulations. The information is also used in searches for similar crimes and patterns in other cases, and to more effectively assess workload, organizational structure, alignment of duties, required staffing, and necessary resources.

No.	Question	Response
1.4	How is the information provided to FHFA-OIG?	Information is provided to FHFA-OIG from individuals through email, regular mail, and FHFA-OIG's website Hotline form, as well as FHFA-OIG Hotline telephone staff. Other information is collected by FHFA-OIG investigative staff through personal or telephonic interviews and other investigative activities.
1.5	Given the amount and type of information collected, what are the risks to an individual's privacy that are associated with collection of the data? Explain in detail how the loss or compromise of the information will/can affect an individual's privacy.	Risks to an individual's privacy are that personal, financial, and other sensitive information may be improperly disclosed or compromised. There is also a risk that unauthorized persons may learn that an individual is the subject of or associated with a criminal or civil investigation by FHFA-OIG or other law enforcement entity.
1.6	Are Social Security numbers collected or used in the system?	Yes.
1.7	If Social Security numbers are being collected, provide the legal authority for the collection. In addition, describe in detail the business justification for collecting SSNs, what the consequences would be if SSNs were not collected, and how the SSNs will be protected while in use, in transit and in storage.	The Inspector General Act of 1978 and the Inspector General Empowerment Act of 2016 authorize the collection of Social Security numbers (SSNs) for law enforcement investigations. SSNs are often necessary in the law enforcement context to reliably identify investigation subjects and witnesses. The consequence of not collecting SSNs is the potential misidentification of an individual or witness in the course of an investigation, which could undermine the reliability and integrity of the investigation, and result in inefficiency and potential errors concerning vital criminal evidence. SSN data is protected in accordance with NIST 800-53, FIPS 199, other relevant NIST information security standards, and Special Publications.

Section 2.0 Uses of the Information

The following questions delineate the use of information and the accuracy of the data being used.

No.	Question	Response
2.1	How will the information be used and for what purpose?	See Section 1.3.
2.2	Describe the types of controls or safeguards in place to ensure that information is only used in the manner for which it was collected.	<p>The CMS is an internal application hosted within the FHFA-OIG network. As such, the CMS inherits the security control implementation pertaining to User Identification and Authentication from the FHFA-OIG network as outlined in section 2.2 of the General Support System (GSS) PIA, dated March 8, 2018.</p> <p>In order to access the CMS, authorized users must first successfully authenticate and establish a secure connection to the FHFA-OIG network (GSS). To accomplish this, a user needs both a security certificate stored on his or her PIV card, as well as a unique security PIN allowing access to an FHFA-OIG-issued computer.</p> <p>CMS uses Microsoft Integrated Windows Authentication to identify and authenticate application users. Integrated Windows Authentication uses the security features of Windows clients and servers. Unlike other forms of authentication, it does not initially prompt users for a username and password. The current Windows user information on the client computer is supplied by the web browser through a cryptographic exchange with the Web server. If the authentication exchange fails to identify the user, the web browser will prompt the user for a Windows user account name and password prior to granting the user access to the CMS application.</p>

Section 3.0 Retention

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

No.	Question	Response
3.1	How long is the information retained?	FHFA-OIG's OI Policies and Procedures Manual, Chapter 5) provides the procedures for preserving the records and information maintained in CMS. The FHFA-OIG Records Management Policy and the incorporated FHFA Comprehensive Records Schedule (CRS) control the retention and disposition of information and records in CMS. All records and information in CMS will be retained in accordance with the above policies and CRS.
3.2	Has a retention schedule been approved by FHFA's Records Management Office and NARA? If yes, provide the corresponding GRS or FHFA specific Records Schedule number.	FHFA-OIG records are addressed in sections 5.3 and 7.2 of FHFA's Comprehensive Records Schedule. The NARA Authority for the FHFA Comprehensive Records Schedule is N1-543-11-1, as approved on January 11, 2013, and reflects GRS Transmittal No. 31, dated April 1, 2020.

3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	<p>For the short-term, the risks remain the same as described above in section 1.5. The risks are mitigated by limiting and controlling access, as described above in section 2.2. Permissions will be required to access the data and will not be granted without appropriate need-to-know and training. Access will be quickly terminated for employees when no longer needed or when no longer appropriate.</p> <p>For case files requiring a longer retention period, there is a risk that technology will change, resulting in the need for a different or enhanced approach to system security. FHFA-OIG mitigates this risk by following the latest NIST, FIPS, and other relevant information security standards to protect its systems and data.</p>
-----	--	---

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 an individual's ability to ensure the accuracy of the information collected about them.

No.	Question	Response
4.1	Has a System of Record Notice (SORN) been created? If so, provide the SORN name and number. If one has not, and one is required, provide the name of the SORN and the expected publication date in the Federal Register.	Yes. FHFA-OIG published an updated SORN on March 9, 2021, in the Federal Register (86 Fed. Reg. 13548). The SORN includes the FHFA-OIG Investigative Files Database (FHFA-OIG-2) as well as FHFA-OIG Investigative Document Repository MIS Database (FHFA-OIG-3).
4.2	Was notice provided to the individual prior to collection of information? If so, what type of notice was provided?	No.
4.3	Do individuals have the opportunity and/or right to decline to provide information? What are the consequences if an individual declines to provide the information?	Hotline complainants have the option to remain anonymous and not provide personal information. In contrast, subjects or targets of investigation, witnesses, and others generally do not have this option. There are no direct consequences to a Hotline complainant who declines to provide information; indirectly, the choice to withhold information may adversely affect the quality of the investigation.
4.4	What are the procedures that allow individuals to gain access to their information?	FHFA has issued Freedom of Information Act (FOIA) and Privacy Act regulations that address the production and release of FHFA-OIG records. FHFA-OIG independently has adopted processes, posted on the FHFA-OIG public website, for individuals to request records under FOIA and the Privacy Act.

No.	Question	Response
4.5	What are the procedures for correcting inaccurate or erroneous information?	<p>Office of Investigations employees are responsible for ensuring the information in CMS is current and accurate.</p> <p>Procedures allowing individuals to access and correct records are set forth in FHFA-OIG's SORN. As stated in the SORN, Office of Investigation systems of records contain certain records that are exempt from the notification, access, and contesting records requirements pursuant to the provisions of 5 U.S.C. 552a(j)(2), (k)(2), and (k)(5).</p>

Section 5.0 Sharing and Disclosure

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

No.	Question	Response
5.1	With which internal organization(s) is the information shared? What information is shared and for what purpose?	Information may be shared with other FHFA-OIG offices as needed to further OIG audit, evaluation and counsel activities. Audit, evaluation, and other OIG personnel will ensure that efforts are not duplicated, and that law enforcement activity and individuals' privacy are not compromised by inadvertent disclosure during the conduct of an audit, evaluation or other matter.
5.2	With which external organization(s) is the information shared? What information is shared, and for what purpose? External organization(s) include Federal, state and local government, and the private sector.	Information may be shared with other law enforcement agencies, including the Department of Justice, state prosecutors, and state and federal law enforcement agencies (including other OIGs) for the purpose of criminal investigation and prosecution. Other releases may be made in connection with litigation, or to members of the general public and media in response to FOIA requests, but only as appropriate and in accordance with the personal privacy protections in the FOIA statute (5 U.S.C. § 552(b)).
5.3	Is the sharing of PII outside FHFA-OIG compatible with the original information collection? If so, is it covered by an appropriate routine use in a SORN? Describe such use. If not, describe the legal authority that permits PII to be shared outside of FHFA-OIG.	Yes. FHFA-OIG shares information in the CMS in accordance with the routine uses set forth in FHFA-OIG's published SORN .

No.	Question	Response
5.4	<p>Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.</p>	<p>Risks to an individual's privacy are that personal, financial, and other sensitive information may be improperly disclosed or compromised. There is also a risk that unauthorized persons may learn that an individual is the subject of or associated with a criminal or civil investigation by FHFA-OIG or other law enforcement entity.</p> <p>Case information from the CMS may be shared with other federal and state law enforcement entities, as described above. No outside law enforcement entities have access to CMS. Risks to individuals' privacy are mitigated by the use of encryption to protect data in transit and at rest. Such processes are in accordance with the protections applied to the GSS. Data in transit is protected via network protocols encrypted with transport layer security, and data at rest is protected via database encryption.</p> <p>Releases may also be made to members of the general public or media in response to FOIA requests. Risks to individuals' privacy are mitigated by reviewing the information before release and withholding or redacting information in accordance with personal privacy exemptions in the FOIA statute and FHFA implementing regulations.</p>

Section 6.0 Technical Access and Security

The following questions describe technical safeguards and security measures.

No.	Question	Response
6.1	What procedures are in place to determine which users may access the System? Are these procedures documented in writing?	<p>Access to the CMS is restricted to authorized users. Those authorized users are identified by the Deputy Inspector General for Investigations (DIGI), and are limited to Special Agents, counsel, OI management, investigative support staff, and other OIG personnel with demonstrated need for access as approved by the DIGI. Access procedures are documented in writing in the OI Policy and Procedures Manual (Section 5.14).</p> <p>Access to a case file is on a “need to know” basis and is restricted to OI and other limited FHFA-OIG staff and contractors who need to access case information (i.e., case agent, SAC, Operations Officers, and OI management). With the exception of investigations designated and identified as “Confidential,” all OI staff have read-only access to information contained in the CMS.</p>

No.	Question	Response
6.2	<p>Will non-FHFA-OIG personnel (e.g. contractor personnel, regulated entity personnel) have access to the System and information contained therein? If yes, how will they gain access to the System? How will FHFA-OIG control their access and use of information? Are there procedures documented in writing?</p>	<p>Non-FHFA-OIG personnel generally do not have access to the CMS. The only exception is for contractor staff assigned to support the OI Hotline. However, these persons have limited access, and only by secure means. Contractors (including hotline operators) sign a non-disclosure agreement, require an FHFA-OIG Active Directory account, and must be issued an FHFA-OIG workstation prior to gaining access to CMS. They first must login to the FHFA-OIG network using two-factor authentication (such as an HSPD-12/PIV card) before they can access CMS. The CMS runs additional checks to ensure that the FHFA-OIG logged-in user has the required permissions to access the CMS data in question. Future needs will determine any changes to the access policy, and all changes will be approved by the Deputy Inspector General for Investigations. Procedures are documented in the Office of Investigations manual.</p>
6.3	<p>Describe the type and frequency of training that is provided to users either generally or specifically that is relevant to the program or System.</p>	<p>CMS user training is conducted upon assignment to the Office of Investigations and lasts approximately 3 hours. This training includes assignments of access and log-on information. Users are also trained on how to access information safely and securely in the CMS. Ongoing CMS training is conducted as needed. In addition, all FHFA-OIG employees must complete, as an annual training requirement, courses on Information Security Awareness, the FHFA-OIG IT Policy, and the FHFA-OIG IT Procedures and Rules of Behavior.</p>
6.4	<p>Describe the technical/administrative safeguards in place to protect the data.</p>	<p>See section 2.2 for detailed technical information on controls and safeguards to protect the data.</p>

6.5	What auditing measures are in place to protect the data? Who reviews these measures and how frequently are they reviewed?	Local server audit logs, as well as audit logs specific to the CMS software itself, compliment the auditing measures in place to protect the FHFA-OIG GSS. CMS automatically sends email notifications to the IT administrator when there is an error or an unauthorized access attempt. The IT administrator reviews the CMS audit logs pertaining to the aforementioned incidents upon receipt of the email notification.
6.6	Has a Security Assessment and Authorization (SA&A) been completed for the System or Systems supporting the program? If so, provide the date the last SA&A was completed. If not, and one is required, provided the expected completion date of the SA&A.	The CMS was included in the SA&A of the third-party infrastructure previously hosting the system, and a new SA&A has been completed for the CMS application hosted within the FHFA-OIG infrastructure. The CMS application SA&A was completed on May 26, 2022. The most recent annual SA&A of the supporting FHFA-OIG GSS was completed on December 17, 2024.
6.7	Has an Authority to Operate (ATO) been issued for this System? If so, what date was it issued, and for how long was it issued? Provide a copy to the Chief Counsel with this PIA. If not, when do you anticipate such ATO being issued?	An initial Authority to Operate (ATO) and ongoing authorization was issued for CMS on May 26, 2022. The ATO decision is reviewed annually as part of the annual CMS Security Assessment Plan. The last ATO was signed on December 18, 2024. The security authorization of the information system will remain in effect until the completion of the next annual assessment and subsequent authorization decision, in alignment with Office of Management and Budget Circular A-130.

Signatures

FHFA-OIG:

Kimberly P. Davis
System Owner

**KIMBERLY
DAVIS**
System Owner (Signature)

Digitally signed by
KIMBERLY DAVIS
Date: 2025.07.07
15:39:51 -04'00'

July 7, 2025
Date

Paul Conlon
Executive Sponsor

Amanual Estefou
System Developer

Michael Stoner
Chief Information Security Officer


Michael Smith
Chief Information Officer

Mary B. Schaefer
Acting Chief Counsel

FHFA:

Brent Burris
Senior Agency Official for Privacy
(Printed Name)

PAUL
CONLON

 Digitally signed by PAUL
CONLON
Date: 2025.07.08
07:08:45 -04'00'


Executive Sponsor (Signature)

AMANUAL
ESTEFOU

 Digitally signed by
AMANUAL ESTEFOU
Date: 2025.07.07
15:53:23 -04'00'

System Developer (Signature)

MICHAEL
STONER

 Digitally signed by
MICHAEL STONER
Date: 2025.07.08
08:24:35 -04'00'


Chief Information Security Officer
(Signature)

MICHAEL
SMITH

 Digitally signed by
MICHAEL SMITH
Date: 2025.07.08
08:40:39 -04'00'

Chief Information Officer
(Signature)

MARY
SCHAEFER

 Digitally signed by MARY
SCHAEFER
Date: 2025.07.08
08:46:43 -04'00'

Acting Chief Counsel
(Signature)

BRENT
BURRIS

 Digitally signed by
BRENT BURRIS
Date: 2025.07.14
12:03:45 -04'00'

Senior Agency Official for Privacy
(Signature)

July 8, 2025

Date

July 7, 2025

Date

July 8, 2025

Date

July 8, 2025

Date

July 8, 2025

Date

July 14, 2025

Date