Privacy Impact Assessment

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

07/05/2022
DATE

FHFA-OIG's Chief Counsel handles certain tasks commonly undertaken by an agency's Senior Agency Official for Privacy (SAOP). This template is used when FHFA-OIG's Chief Counsel determines that an FHFA-OIG IT System contains Personally Identifiable Information and a more in-depth assessment is required.

Complete and sign this template and forward to the FHFA-OIG Chief Counsel for review and coordination with the agency SAOP.

Guidance for Completing the Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is an analysis of how Personally Identifiable Information (PII) is collected, stored, maintained, and shared. A PIA must be completed when FHFA-OIG: 1) develops or procures an IT System or project that collects, maintains, or disseminates PII from or about members of the public; or 2) initiates a new electronic collection of PII for 10 or more members of the public. System Owners are primarily responsible for completing the PIA with assistance from FHFA-OIG's IT developers, IT security officers, and Office of Counsel.

Below is guidance, by section, for a System Owner to follow when completing a PIA.

OVERVIEW SECTION

- Provide a thorough, complete, and clear overview of the System and give the reader the appropriate context to understand the responses. Some questions to considerinclude:
  - What is the purpose of the System?
  - What will be the primary uses of the System?
  - How will this support the Division's/Office's/Program'smission?
- This section fulfills the E-Government Act's requirement for an introduction to members of the public who may be reading the PIA. PIAs may be made publicly available unless a determination is made to not make the PIA available because publication would raise security concerns and/or reveal classified or sensitive information.

FOR A FULL PIA

- **COMPLETE ALL SECTIONS**

FOR A MODIFIED PIA - Under certain circumstances the FHFA-OIG Chief Counsel may make a determination that a complete PIA is not necessary depending upon the nature and extent of the PII collected. When the Chief Counsel makes such a determination, the System Owner only needs to complete the following sections of the PIA template:

- **OVERVIEW**
- **SECTIONS 1, 2, AND 6**

SECTION 1.0 CHARACTERIZATION OF THE INFORMATION

- Identify if the System contains information about individuals, versus statistical, geographical, or financial information, with no link to a name or other identifier, such as, home address, social security number, account number, home, mobile or facsimile telephone number, or personal e-mail address.
- Examples of sources of the information include information that comes from an individual applying for a loan or mortgage, or other forms that an individual completes. A question toconsider:
  - Where does the data originate? (e.g., FHFA, Office of Personnel Management, Regulated Entities, other Financial Institutions, or third parties). A third party is usually a non-Federal person or entity, which may be a source of data/information (e.g., a bank, an internet service provider, or a private organization).
- If the System collects information from 10 or more members of the public, ensure that FHFA-OIG has received prior approval from OMB to do so or determine whether OMB's approval is needed to collect the information in accordance with the Paperwork Reduction Act. If you are unsure of this last requirement, contact the FHFA-OIG Office of Counsel forassistance.

SECTION 2.0 USES OF THE INFORMATION

- Identify the primary uses of the information and how the information supports FHFA-OIG's mission.
- Identify the controls that are in place to ensure the information will be used for the manner for which it was collected. For example, access to the information will be restricted to a limited number of staff who use the data for their specific programuse.

SECTION 3.0 RETENTION

- The Privacy Act requires an agency to address the retention and disposal of information about individuals. This retention information is published in the Privacy Act System of Record Notice (SORN).
- The retention periods for data/records that FHFA-OIG manages are contained in either the National Archives and Records Administration (NARA) General Records Schedule (GRS) or FHFA's Records Schedule, to which FHFA-OIG is subject. For the data being created/ maintained in the System, these records schedules are the authoritative sources for this information. For assistance, contact FHFA-OIG's Office of Administration(OAd).
- Disposing of the data at the end of the retention period is the last state of life-cycle management. Records subject to the Privacy Act have special disposal procedures (e.g. shredding of paper documents).

SECTION 4.0 NOTICE, ACCESS, REDRESS AND CORRECTION

- The Privacy Act requires that "each agency that maintains a System of records shall maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President." 5 U.S.C. 552a(e)(1).
- Data can be retrieved in a number of ways, but there is usually a personal identifier associated with a record. If the System retrieves information by an individual's name or other unique identifier (e.g. social security number) it is a Privacy Act System and will need a SORN published in the Federal Register. The System may already have a Privacy Act SORN. If you do not have a published SORN, or are unsure whether one exists, contact FHFA-OIG's Office ofCounsel.
- If a name or other unique identifier is not used to retrieve information, it is possible that the System is not a Privacy Act System. However, even though information may not fall under the Privacy Act's protection and requirements, certain information may still be protected from disclosure under the Freedom of Information Act.
- FHFA-OIG is subject to FHFA's agency specific Privacy Act Rule published in the Federal Register (12 CFR Part 1204) that explains how individuals can gain access to information about themselves and correct errors, ifappropriate.
- Any employee who knowingly and willfully maintains a System of Records without meeting the Privacy Act notice requirements (5 U.S.C. 552a(e)(4)) is guilty of a misdemeanor and may be fined up to $5,000.

SECTION 5.0 SHARING AND DISCLOSURE

- If you do not know whether or not Systems share data, contact either the business owner of the data, or the IT specialist who knows what interfaces exist between the Systems/applications. As an example, if your System/application shares data with another System/application, ask yourself

whether you have access to the data in the interfaced System/application. If so, then your answer is yes and an explanation is needed.

- Also consider "other" users who may not be obvious as those listed, such as GAO. "Other" may also include database administrators or IT Security Officers. Also include organizations listed in the Privacy Act SORN under the "Routine Use" section when a Privacy Act SORN is required. The more comprehensive the list, the better it is.
- You must first review the SORN to determine whether any information that may come from an existing SORN allows that information to be exchanged and used for these new purposes or uses. There are restrictions on the use and disclosure of information that are set forth in a SORN.

SECTION 6.0 ACCESS AND SECURITY

- Access to data by a user (i.e. employee or contractor personnel) within FHFA-OIG is determined on a "need-to-know" basis. This means to authorized employees or contractor personnel who have a need for the information to perform their duties may be granted access to the information. Factors to consider in making this determination include the user's job requirements including supervisory responsibilities.
- The criteria, procedures, controls and responsibilities regarding access must be documented in order to comply with the intent of the Federal Information Security Management Act of 2002 for standards and guidelines on security and privacy.
- The System owner is responsible for ensuring that access to information and data is restricted to authorized personnel. Usually, a user is only given access to certain information that is needed to perform an official function. Care should be given to avoid "open Systems" where all information can be viewed by all users. System administrators may be afforded greater access – i.e. to all of the data – depending upon the System and/or application. However, restrict access when users do not need to have access to all the data.
- When a contract provides for the operation of a System on behalf of FHFA-OIG, the Privacy Act requirements must be applied to such a System. Contact the Contracting Officer or Contracting Officer's Representative to determine whether the contract contains the Privacy Act clause and the requirements thereunder.
- The Security Assessment and Authorization (SA&A) process requires a System security plan that identifies the technical controls associated with identification and authentication of users. Certain laws and regulations require monitoring of Systems to ensure that only authorized users can access the System for authorized reasons. In doing so, consider what controls are in place to ensure that only those authorized to monitor the System can in fact monitor use of the System. For example, business rules, internal instructions, and posting Privacy Warning Notices address access controls and violations for unauthorized monitoring. System Owners are responsible for ensuring that no unauthorized monitoring is occurring.
- The IT Security Plan describes the practice of applying logical access controls. Logical access controls are System-based means by which the ability to access a System is either explicitly enabled or restricted. System Owners are responsible for ensuring that no unauthorized access is occurring.
- The IT Security Plan describes the practice of audit trails. An audit trail maintains a record of System activity and user activity including invalid logon attempts, access to data and monitoring. The SA&A process requires a System security plan outlining the implementation of the technical controls associated with identification and authentication.
- Every System/application/process that uses data must have controls in place to prevent the misuse of the data by those having access to the data.
- All employees, including contractors, have requirements for protecting information in Privacy Act Systems. Describe the controls in place, including any privacy and security awareness controls such as training materials, to protect the information.

PIA FORM

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: 07/05/2022

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.

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 transition of its CMS from third-party hosting to FHFA-OIG infrastructure.

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.

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.

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.

#	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.

#	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.

#	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.	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. 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. 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.

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?	Pursuant to the FHFA-OIG Records Management Policy (dated March 14, 2014) and the incorporated FHFA Comprehensive Records Schedule (dated January 1, 2013), Significant Investigative Case Records (as defined in the Schedule) are retained permanently. The records are transferred to NARA 30 years after cutoff. Cutoff occurs when the investigative activity is completed or superseded. All other Investigative Case Records are deemed temporary, and either destroyed or deleted 15 years after cutoff. Investigative Non-Case Records are deemed temporary and are destroyed or deleted three years after cutoff.
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 section 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.	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. 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.

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.

#	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 generallydo 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.

#	Question	Response
4.5	What are the procedures for correcting inaccurate or erroneous information?	Office of Investigations employees are responsible for ensuring the information in CMS is current and accurate. 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).

Section 5.0 Sharing and Disclosure

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

#	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. https://www.govinfo.gov/content/pkg/FR-2021-03-09/pdf/2021-04796.pdf

#	Question	Response
5.4	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	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. 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. 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.

Section 6.0 Technical Access and Security

The following questions describe technical safeguards and security measures.

#	Question	Response
6.1	What procedures are in place to determine which users may access the System? Are these procedures documented in writing? **If so, provide a signed copy to the Chief Counsel with this PIA.**	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). 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.

#	Question	Response
6.2	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? **If so, provide a copy to the Chief Counsel with this PIA.**	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.
6.3	Describe the type and frequency of training that is provided to users either generally or specifically that is relevant to the program or System.	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.
6.4	Describe the technical/administrative safeguards in place to protect the data.	See section 2.2 for detailed technical information on controls and safeguards to protect the data.
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.

#	Question	Response
		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 March 31, 2022.
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?	A new Authority to Operate (ATO) and ongoing authorization was issued for CMS on May 26, 2022. 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 (Printed Name)	KIMBERLY DAVIS Digitally signed by KIMBERLY DAVIS Date: 2022.07.05 16:20:22 -04'00' System Owner (Signature)	7/5/22 Date
Paul Conlon Executive Sponsor (Printed Name)	PAUL CONLON Digitally signed by PAUL CONLON Date: 2022.07.05 16:17:50 -04'00' Executive Sponsor (Signature)	07/05/2022 Date
Amanual Estefou System Developer (Printed Name)	AMANUAL ESTEFOU Digitally signed by AMANUAL ESTEFOU Date: 2022.07.05 16:30:05 -04'00' System Developer (Signature)	07/05/2022 Date
Michael Stoner Chief Information Security Officer (Printed Name)	MICHAEL STONER Digitally signed by MICHAEL STONER Date: 2022.07.05 16:46:20 -04'00' Chief Information Security Officer (Signature)	07/05/2022 Date
Michael Smith Chief Information Officer (Printed Name)	MICHAEL SMITH Digitally signed by MICHAEL SMITH Date: 2022.07.13 16:43:14 -04'00' Chief Information Officer (Signature)	07/13/2022 Date
Stacey Nahrwold Acting Chief Counsel (Printed Name)	STACEY NAHRWOLD Digitally signed by STACEY NAHRWOLD Date: 2022.07.13 18:12:22 -04'00' Acting Chief Counsel (Signature)	07/13/2022 Date

FHFA:

Tasha Cooper Senior Agency Official for Privacy (Printed Name)	TASHA COOPER Digitally signed by TASHA COOPER Date: 2022.07.14 21:59:31 -04'00' Senior Agency Official for Privacy (Signature)	Date