Privacy Impact Assessment (PIA)

SMARSH MOBILE GUARD

December 2025
Date

System/Collection Overview
FHFA staff and authorized contractors are provided agency-managed mobile devices. The Smarsh MobileGuard system (MobileGuard) receives near real time copies of short message service (SMS) text message traffic directly from the agency-managed mobile device carriers (Verizon and AT&T Wireless). From there, the SMS text messages can be exported and downloaded to FHFA's eVault system for storage in accordance with records retention requirements.

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 System/Collection being procured or developed. The questions address all information collected, with emphasis on the collection of personally identifiable information (PII), such as name, address, social security number, date of birth, financial information, etc.

#	Question	Response
1.1	What information types (e.g., contact information, demographic information, employment information) are being collected, used, disseminated, or maintained in the System/Collection?	The system natively collects the phone numbers from SMS text messages, including the number receiving the text and the number sending the text. The system also collects the content of the text messages.
1.2	What or who are the sources of the information provided to FHFA and included in the System/Collection?	The SMS text messages are received directly from the wireless carrier (AT&T and Verizon Wireless) for the agency-managed mobile device. The internal FHFA contact information is obtained via FHFA's Active Directory stored in MobileGuard.
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	To ensure SMS text communications to/from FHFA-managed mobile devices are stored in an alternate location other than the mobile device and accessible for agency needs, such as litigation.
1.4	How is the information provided to or otherwise obtained by the System/Collection?	The wireless carriers send a near real time copy of all SMS text messages sent to/from a registered FHFA-managed mobile device to the MobileGuard system. MobileGuard on a batch basis sends messages to an FHFA Exchange email, which is ultimately imported into FHFA's eVault system.

1.5	Are Social Security Numbers (SSNs) being collected or used in the System/Collection? • If yes, describe in detail: 1) The business justification for collecting or using SSNs; 2) The consequences if SSNs are not collected or used; and 3) How the SSNs will be protected while in use, in transit and in storage. • If no, state "N/A" in the response section.	N/A

Section 2.0 Uses of the Information

The following questions delineate the use of information.

#	Question	Response
2.1	How will the information be used and for what purpose?	The primary purpose for this collection is to support agency litigation-related needs, such as litigation-hold requests and/or eDiscovery searches.
2.2	Describe any types of measures or processes in place to ensure that information is only used in the manner for which it was collected.	Only authorized administrators will have access to the MobileGuard portal. Single Sign On and logging services are used as documented in the FHFA MobileGuard Customer Controls. SMS text messages forwarded to the Exchange/eVault are accessible only to Exchange/eVault administrators.

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?	The records are temporary and can be destroyed upon creation or update of the final record, or when no longer needed for business use, whichever is later. As a matter of business practice, messages and the associated phone numbers are retained in the system for seven years from the date the message was sent or received. Messages transferred to FHFA's eVault system are retained in accordance with the records schedule applicable to the FHFA employee or contractor who sent/received the message.
3.2	Has a retention schedule been approved by FHFA's Records Management Office and National Archives and Records Administration (NARA)? If yes, provide the corresponding General Record Schedule (GRS) or FHFA specific Records Schedule number.	Yes, for messages in the MobileGuard system, GRS 5.2, Item 020 – Intermediary Records (DAA-GRS-2022-0009- 0002) is the applicable retention schedule.

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

#	Question	Response
4.1	Is the information in this System/Collection retrieved by an individual's name or personal identifier such as an SSN or other identification? • If no, please put "no" in the Response section. • If yes, the System/Collection will need to be covered by a Privacy Act System of Records Notice(s) (SORN(s)). Please provide the SORN(s) name and number or indicate that a SORN is in progress.	No, and therefore no SORN is required because MobileGuard does not create a system of records, as defined by the Privacy Act of 1974 (5 USC 552a).
4.2	How is notice about the collection of PII provided to individuals prior to the collection for the System/Collection (e.g., direct notice, Privacy Act Statement or public notice, SORN)? If notice is not provided, explain why not.	N/A. Information is obtained from the FHFA Active Directory and from the wireless carriers associated with agency-managed mobile devices and is not directly collected from individuals. However, FHFA staff who have been issued an agency-managed mobile device are routinely notified by the wireless carriers that text and picture messages sent to and from their agency-provided device are shared with FHFA.
4.3	Is an individual's response to the request for information voluntary or mandatory?	NA. Information is obtained from the FHFA Active Directory and from the wireless carriers associated with the agency-managed mobile devices and is not directly collected from individuals.
4.4	What are the consequences if an individual declines to provide the information?	NA. Information is obtained from the FHFA Active Directory and from the wireless carriers associated with the agency-managed mobile devices and is not directly collected from individuals.
4.5	What are the procedures that allow individuals to gain access to their information?	N/A. The system is not a Privacy Act system of records and as such, individuals have no right of access to the information in the system.
4.6	What are the procedures for correcting inaccurate or erroneous information?	N/A. The system is not a Privacy Act system of records and as such, individuals have no right to correct inaccurate or erroneous information.

Section 5.0 Sharing and Disclosure

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

#	Question	Response

5.1	Is information shared with internal office(s) or division (s)? • If yes, please identify the FHFA office(s) or division(s) and describe the information shared and for what purpose. • If no, please state "N/A" in the response section.	Information is shared with the Office of the Chief Information Officer (OCIO) and the Office of the General Counsel (OGC) for the purpose of retaining communications to respond to a litgation hold or eDiscovery request and to secure the retained information for such purposes.
5.2	Is information shared with external (outside FHFA) agencies, organizations, contractors, or other entities? For purposes of this Section, external organization(s) include Federal, state, and local government, and the private sector. • If yes, please identify the information shared, and for what purpose. • If no, skip to Section 6.	Information is not routinely shared with external parties. However, as with all FHFA information, information from MobileGuard may be shared with third parties if required by law (e.g., disclosures made pursuant to litigation).
5.3	Is the sharing of PII outside the agency compatible with the stated purpose of the original information collection? • If yes and a SORN applies, identify the applicable routine uses in the SORN listed in Question 4.1. • If no and/or a SORN does not apply, identify the legal authority that permits the sharing outside FHFA.	Yes, the external sharing of this information is compatible with the original purpose for this information collection and is authorized by 12 U.S.C. 4513(a)(2)(B), and 44 U.S.C. 3101. No SORN applies because no "system of records," as defined by the Privacy Act (5 USC 552a), is created.

Section 6.0 Technical Access and Security

The following questions describe technical safeguards and security measures.

#	Question	Response
6.1	Will FHFA Office of Inspector General (OIG) or non-FHFA personnel (e.g., contractor personnel, regulated entity personnel) have access to the System/Collection and information contained therein? • If yes, how will they gain access to the System/Collection? • If no, how will the agency control access to and use of that information? • Are there procedures or criteria documented in writing? If so, please describe.	OCIO and OGC contractors with an official business need to administer or search the SMS text messages will have access. Access to the information on the MobileGuard portal must be approved by the System Owner and follow the procedures defined in the Customer Controls. SMS text messages forwarded to the Exchange/eVault are accessible only to Exchange/eVault administrators.
6.2	Are there any conflicts of interest with respect to the System/Collection or information? If so, identify the conflicts of interest and describe how they are addressed.	No.
6.3	Describe the type and frequency of training that is provided to users that is specifically or generally relevant to the System/Collection.	All FHFA employees and contractors with access to FHFA's network are required to undergo security, privacy, and Records and Information Management training for use of FHFA systems at

		onboarding and annually thereafter. In addition, all FHFA users with elevated privileges receive specialized security training, and role-based privacy awareness training for those individuals whose work duties regularly involve the collection, use, storage, access, or maintenance of PII.
6.4	Describe the technical/administrative safeguards in place to protect the data.	SMS messages are encrypted in transit from the carrier to MobileGuard, from MobileGuard to FHFA and encrypted at rest within MobileGuard. FHFA has developed Customer Controls that describe the agency's implementation of controls designated as the responsibility of the customer agency. This includes procedures for securely managing access to the system, reviewing audit logs, etc.

Section 7.0 Risk

The following questions describe the risk to the information within the System or Collection.

#	Question	Response
7.1	Given the amount and type of information collected, what are the risks to an individual's privacy associated with collection of the data? Explain in detail how the loss or compromise of the information will/can affect an individual's privacy and describe how these risks are mitigated.	If the data collected were compromised or lost, at a minimum, the phone numbers of the senders/receivers would be exposed as well as the content of the SMS texts, which could compromise the privacy and confidentiality of the employee or any individual described in the SMS text and potentially cause that employee or individual embarrassment or risk of blackmail or identity theft, as well as potentially disclose sensitive FHFA information. However, this risk is limited as FHFA staff are informed and routinely reminded that they have no expectation of privacy when using agency resources such as FHFA-issued mobile devices. Likewise, communications from third parties should be work-related in nature, thereby limiting privacy risks. Risks related to breaches of the information are further mitigated via the security measures described herein.
7.2	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	The risks associated with the length of retention are relatively low given the moderate retention period of seven years. Risks are limited by limiting access to the system and properly disposing of the information at the end of the retention period.

7.3	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	Information from the MobileGuard system is not routinely shared with external parties, thereby limiting privacy risks. These risks are mitigated by limiting any external sharing to that which is authorized by law. Additional risk mitigations may include seeking protective orders before courts or administrative bodies overseeing matters in litgation and notifying external recipients of information's protected status, if applicable (e.g., if the information qualifies as Controlled Unclassified Information).