
**Privacy Impact Assessment (PIA) Template**

Cisco Meraki Mobile Device Management (Meraki)

August 23, 2023

| System/Collection Overview |
| --- |
| Cisco Meraki Mobile Device Management (Meraki) is an existing information system used by the Office of Technology and Information Management (OTIM) to track and manage Apple iOS (iPhone and iPad) mobile devices issued to FHFA employees and contractors for business use. The management capabilities include configuring iOS devices with security profiles to ensure a consistent look/feel and security configuration across all devices, the ability to locate lost or missing devices, and the ability to remotely lock or wipe a device to protect agency data. Meraki is operated internally by FHFA employees and contractors. |

**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 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? | Business contact information, device identifiers, and geospatial or geolocation information. |
| 1.2 | What or who are the sources of the information provided to FHFA and included in the System/Collection? | Names and business email addresses are obtained from Active Directory (AD). Business phone numbers are assigned in the system as provided by the telephone carrier. Internet Protocol (IP) addresses and geospatial and geolocation information are identified by the system during normal use. |
| 1.3 | For what purpose is the information being collected, used, disseminated, or maintained? | To identify who has been assigned a particular device and to manage that device. |
| 1.4 | How is the information provided to or otherwise obtained by the System/Collection? | When an iPhone or iPad is issued to a user, AD is consulted to obtain the name and email address of the user. The telephone carrier assigns the phone number to the issued iPhone. The IP address and geospatial or geolocation information are provided by the assigned device. |
| 1.5 | Are Social Security Numbers (SSNs) being collected or used in the System/Collection?<br>• If yes, describe in detail:<br>1) The business justification for collecting or using SSNs;<br>2) The consequences if SSNs are not collected or used; and<br>3) How the SSNs will be protected while in use, in transit and in storage.<br>• 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? | To identify who has been assigned a particular device and to manage that device. |

| | | |
|---|---|---|
| 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. | Access is limited to administrators. Administrative accounts and logs are reviewed on a quarterly basis to identify unauthorized activity. All administrative staff sign an annual Rules of Behavior agreement, which requires, in relevant part, all users to use FHFA information systems, hardware, software, and information only for lawful, official, and permitted purposes and that such be consistent with the *Standards of Ethical Conduct for Employees of the Executive Branch*, 5 C.F.R. Part 2635. |

**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? | Information in Meraki is temporary and will be destroyed or deleted when there is no longer a business use for that information *(i.e., when a device is no longer assigned to a user and is returned by that user to FHFA).* |
| 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. | The information retained in Meraki is subject to FHFA Comprehensive Records Schedule Item 6.4 Transitory Records: Records of short-term interest that have minimal documentary or evidential value, including but not limited to, routine notifications of meetings, routine requests for publications and copies of replies which require no administrative action, transmittal information that does not add any information to that contained in the transmitted materials, to-do lists that serve as reminders, and extra copies of documents when the record copy is filed in the agency recordkeeping system. |

**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?<br>• If no, please put "no" in the Response section.<br>• 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. | Yes, information in this system can be retrieved by a search using a user's name. However, such a search only retrieves information about the device, does not retrieve any additional information about the user, and therefore does not retrieve information about the individual, as required by the Privacy Act definition of "record." Accordingly, the Privacy Act does not apply to this information system. |
| 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. | This system is not the point of original collection of this data and therefore no notice is provided. |

| | | |
|---|---|---|
| 4.3 | Is an individual's response to the request for information voluntary or mandatory? | N/A |
| 4.4 | What are the consequences if an individual declines to provide the information? | N/A |
| 4.5 | What are the procedures that allow individuals to gain access to their information? | The device contains the same information as in the system and thus is readily and immediately available to each user via the assigned device. A user may submit a request to the help desk for geospatial or geolocation information when a device is lost, stolen, or misplaced. |
| 4.6 | What are the procedures for correcting inaccurate or erroneous information? | When a user becomes aware that his or her name is incorrectly identified in this information system, which would likely and only occur after the user sends a request to and is provided access by the help desk, that user can then submit a request to the help desk to correct that user's name in Meraki. Notwithstanding, an incorrectly spelled name does not affect in any manner the function of this information system and carries no consequences to the user. |

**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)?<br>• If yes, please identify the FHFA office(s) or division(s) and describe the information shared and for what purpose.<br>• If no, please state "N/A" in the response section. | N/A |

| | | |
|---|---|---|
| 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.<br>• If yes, please identify the information shared, and for what purpose.<br>• If no, skip to Section 6. | No |
| 5.3 | Is the sharing of PII outside the agency compatible with the stated purpose of the original information collection?<br>• If yes and a SORN applies, identify the applicable routine uses in the SORN listed in Question 4.1.<br>• If no and/or a SORN a does not apply, identify the legal authority that permits the sharing outside FHFA. | N/A |

**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?<br>• If yes, how will they gain access to the System/Collection?<br>• If no, how will the agency control access to and use of that information?<br>• Are there procedures or criteria documented in writing? If so, please describe. | No. Additional information about access is contained in the Customer Controls Document for Cisco Meraki, including but not limited to the requirement that a user have a business need-to-know the information. |
| 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 are required to undergo Security, Privacy, and Records and Information Management (RIM) training at new employee onboarding training 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 and responsibilities involve the collection, use, storage, access, or maintenance of PII. |

| | | |
|---|---|---|
| 6.4 | Describe the technical/administrative safeguards in place to protect the data. | Meraki is covered by the Cisco Meraki North America DC1 and DC2 SOC 2 certifications, independently verifying Cisco's conformance with security and privacy requirements of AICPC standards. FHFA has developed Customer Controls that describe the Agency's implementation of controls that are the responsibility of FHFA as the Customer Agency, and not the responsibility of the vendor. This includes the implementation of single sign-on authentication, procedures for securely managing access to the system, assigning permissions based on the concept of least privilege, generating, and 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 a user's data is exposed, they could be subject to harassment or embarrassment. Due to the limited types of PII collected, there is very little, if any risk of identity theft. To prevent unauthorized use of the data, access to the data is limited to those with an official need-to-know and who have signed and are subject to the FHFA System Rules of Behavior and User Acknowledgment. |
| 7.2 | Discuss the risks associated with the length of time data is retained and how those risks are mitigated. | If a user's data becomes exposed, they could be subject to harassment or embarrassment. Due to the limited types of PII collected, there is very little, if any, risk of identity theft. To prevent unauthorized use of the data, access to the data is limited to those with an official need-to-know and who have signed and are subject to the FHFA System Rules of Behavior and User Acknowledgment. |
| 7.3 | Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated. | N/A |