Federal Trade Commission
Privacy Impact Assessment

Mobile Device Management System (MDM)

March 2018

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The FTC Office of the Chief Information Officer (OCIO) operates and maintains the FTC's Information Technology (IT) services, which include the agency's network, servers, applications, databases, computers, and communication facilities. Part of those services include managing the FTC's mobile devices (e.g., smartphones) system by administering and configuring those devices for use by FTC employees and contractors.

The FTC Mobile Device Management (MDM) system includes three separate components that provide wireless services, mobile devices, and configuration and management of the mobile devices to include the application of security controls, monitoring device activity, the distribution of approved applications (apps), and continual performance optimization.

Component 1: MDM is an externally hosted service used to centrally manage FTC issued Mobile Devices and provide the following services:

- Mobile Application management through whitelisting or blacklisting of applications to ensure only authorized use of government-furnished equipment (GFE) to access:
    - Services authorized by the FTC to operate, such as those for email, calendars, and contacts or the FTC intranet as identified in separate PIAs for the HQ Data Center
    - Services authorized by the FTC to use, such as those from government shared services for travel
    - Publicly available services filtered for appropriate use by government staff, similar to the use of URL filters used to limit access to internet sites using FTC-issued laptops or desktops
- Mobile device policy enforcement to alert FTC staff to take action when users lose or attempt to use FTC-issued mobile devices in a manner inconsistent with FTC policy or training through features such as:
    - Remote wipe of a smartphone's contents
    - Forced entry of decryption PIN

Component 2: Mobile Devices, which include their mobile applications and data, are encrypted and then provided by the FTC to authorized users (currently, Mobile Devices are limited to either Apple iPhone or Samsung Galaxy devices). iOS-based devices provide Federal Information Processing Standard (FIPS) 140-2 hardware and data file level encryption. Samsung Android devices provide On Device Encryption (ODE) to include Secure Digital (SD) card and file-level security. Attempts to turn off or remove encryption will render data inaccessible.

Component 3: Wireless Service Provider provides talk, text, and data service for all Mobile Devices for national and international use. The Wireless Service Provider source data is not included in or authorized by any FTC information system; however, the FTC retains and analyzes monthly billing data that it receives to ensure appropriate billing rates are applied to the appropriate Mobile Devices.

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

The legal authority for the collection of this information is defined in:

- Federal Information Security Modernization Act **(**44 U.S.C. § 3551 *et seq.*)
- The FTC Act (15 U.S.C. § 41 *et seq.*)
- 44 U.S.C. § 3101 (records management by agency heads; general duties)

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[1] may be collected or maintained in the system/project. Check all that apply.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.		
☒ Full Name	☐ Biometric Identifiers (e.g., fingerprint, voiceprint)	☒ User ID
☐ Date of Birth	☐ Audio Recordings	☐ Internet Cookie Containing PII
☐ Home Address	☐ Photographic Identifiers (e.g., image, x-ray, video)	☐ Employment Status, History, or Information
☒ Phone Number(s)	☐ Certificates (e.g., birth, death, marriage, etc.)	☐ Employee Identification Number (EIN)
☐ Place of Birth	☐ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☐ Salary
☐ Age	☐ Vehicle Identifiers (e.g., license plates)	☐ Military Status/Records/ ID Number
☐ Race/ethnicity	☐ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	☐ IP/MAC Address
☐ Alias	☒ Geolocation Information	☐ Investigation Report or Database
☐ Sex	☐ Passport Number	☐ Driver's License/State ID Number (or foreign country equivalent)
☒ Email Address		☒ Other *(Please Specify)*: Passwords
☐ Work Address		
☐ Taxpayer ID		
☐ Credit Card Number		
☐ Facsimile Number		
☐ Medical Information		
☐ Education Records		
☐ Social Security Number		
☐ Mother's Maiden Name		

The following types of additional PII may be collected or maintained:

MDM

- Mobile Device profile: Device ID, Mobile Device name, user name, International Mobile Equipment Identifier (IMEI/MEID, used to identify devices on the cellular network)
- Mobile Device location[2]

[1] Per OMB Circular A-130, personally identifiable information (PII) means 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.

[2] MDM does not actively track Mobile Device location but can access current location information, if necessary and authorized, for instance to locate a lost device. To view where a Mobile Device is located, an authorized administrator logs into the MDM console, finds the username associated with the Mobile Device, then clicks on a button to locate the Mobile Device. A program runs to locate that Mobile Device at that point in time. There is no log created or maintained showing the whereabouts of any Mobile Device on a continuous basis.

Mobile Devices

- IMEI/MEID – used to identify devices on the cellular network
- Subscriber Identity Module (SIM) – used by the Wireless Service Provider to authenticate and identify subscribers on their network
- Telephone numbers of incoming and outgoing phone calls
- Telephone numbers of incoming and outgoing text messages

Wireless Service Provider (Mobile Device Billing Data)

The Wireless Service Provider generates and maintains Mobile Device usage details for billing, performance, and functionality purposes, and every month provides to the FTC a CD containing billing data.[3] The billing data includes the name of the employee organization along with other data elements (as specified in 2.2 below).

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

MDM

- Mobile Device profile: manufacturer, model, operating system, installed date, last reported date, mailbox sync status, managed status (whether the mailbox has been appropriately synced), and MDM enrollment status
- Authorized and unauthorized downloaded applications[4]
- Action history: log that tracks compliance status associated with the Mobile Device/user and any actions taken by the system administrator regarding Mobile Devices that are not in compliance with FTC policy

Mobile Devices

- Mobile application data synchronized with source data hosted in other services authorized to use or operate by the FTC such as the HQ Data Center
- Downloaded apps

Wireless Service Provider (Mobile Device Billing Data)

The following information is downloaded from the Wireless Service Provider and retained by the FTC:

- Number of Calls Made/Received
- Number of Minutes Used
- Amount of Data Used
- Number of Texts Sent/Received
- Roaming Charges
- Total Charges in Addition to the Monthly Recurring Charge (MRC)
- Subscriber Total (total charges per user)

[3] The FTC typically does not use the CD[3] and instead accesses billing data via the Provider's online portal. The CD is kept in a locked file cabinet for one (1) calendar year and is then shredded.

[4] Users are encouraged not to download or store any personal information on the Mobile Device, and users are made aware that any information stored by approved apps may be collected by the System and/or Mobile Device.

2.3 What is the purpose for collection of the information listed above?

MDM

- MDM data is necessary for FTC IT staff to manage FTC Mobile Devices.
  - For example, MDM allows staff to keep required applications up-to-date, reset passwords, and proactively secure the Mobile Devices.
  - Additionally, MDM allows staff to secure the devices by initiating and confirming installation of operating system updates and security patches, by preventing users from installing unauthorized applications, and by helping ensure that employees use their FTC-issued Mobile Devices securely and in accordance with FTC policies, procedures, and guidelines regarding privacy, information security, limited personal use, and confidentiality.

Mobile Device

- The information collected on the Mobile Device (See Section 2.1) is necessary for MDM configuration requirements and to support routine use by the authorized Mobile Device user. These configuration requirements and routine uses inform authorized administrators about performance of the Device.

Mobile Device Billing Data

- Monthly billing data is necessary for the FTC to ensure that appropriate billing rates are applied to the appropriate Mobile Devices. Billing information is analyzed and monitored for trends or anomalies as outlined in the FTC Mobile Device Rules of Behavior and FTC policy.

2.4 What are the sources of the information in the system/project? How is the information collected?

Component	***Source of Data***	***Type of Data Provided & How It Is Collected***
MDM	Employee, FTC System Administrator	The information is collected directly from the user when the Mobile Device is registered, from the Mobile Device itself as it is used, or in the case of Mobile Device location, when the "Locate Device" command is sent to the Mobile Device by authorized administrators for authorized purposes. When registering the Mobile Device, the FTC employee is required to create a user profile that allows the Mobile Device to access the FTC's Windows Active Directory.[5] The user profile via Active Directory confirms that the employee is authorized to access his or her network calendar, contacts, and email accounts, and will help ensure the accuracy of data usage information. The system administrator creates a Mobile Device profile for each employee, and the employee enters the applicable passwords and authenticating credentials. The system administrator creates and maintains the catalog of FTC-approved apps.

[5] Active Directory is a centralized database of FTC network users and their authorized levels of permission.

Component	*Source of Data*	*Type of Data Provided & How It Is Collected*
Mobile Device	Mobile Applications	Mobile applications collect data in order to allow users to interact with services authorized for use or operate by the FTC such as those identified within the HQ Data Center.
Mobile Device Billing Data	Wireless Service Provider	The Wireless Service Provider generates billing information for the FTC's use of talk, text, and data on its Mobile Devices on a monthly basis. They then make the electronic billing data available to the FTC.

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
FTC Employees and Contractors	MDM: The FTC limits administrative access to MDM to authorized FTC staff and contractors who provide day-to-day operations and maintenance support (e.g., those who respond to user questions, requests, or incidents). MDM automatically generates a report on the technical status of the Mobile Devices on a weekly basis and emails the report to specific IT staff. Additionally, the FTC has the ability to conduct forensic analysis on MDM System components. For example, if a Mobile Device user installs an authorized application or uses the Mobile Device for any activities outside of the FTC's de minimis policy, authorized FTC staff responsible for managing Mobile Devices may view the downloaded applications and activity for authorized purposes. FTC staff responsible for managing Mobile Devices may also retrieve information about application usage, and the FTC may disclose such information in response to Freedom of Information Act (FOIA) requests, Congressional inquiries, or discovery requests, or for other legitimate business purposes or authorized requests, such as FTC Inspector General (IG) audits and/or investigations.
	Mobile Device: Authorized IT personnel may access information stored on a Mobile Device for authorized purposes or information on stored on services accessed with a mobile device. For example, Help Desk staff may access information on the Mobile Device or on the FTC's email services when assisting users, or IT security staff may perform forensic analysis in response to an incident. The assigned Mobile Device user is the only person who will have daily, routine access to the information on the Mobile Device.
	Mobile Device Billing Data: The FTC restricts access to billing information to authorized FTC employees and contractors who are either responsible for managing Mobile Devices or are explicitly granted access by the contracting officer. The Office of the Chief Information Officer (OCIO) may share billing data with the Financial Management Office (FMO) for budgeting purposes, and also with the Human Capital Management Office (HCMO) and the IG for authorized purposes, as requested or required.
Wireless Service Provider	In accordance with applicable Privacy Act System of Records Notices, MDM system component data necessary to configure, connect, and transmit data to the MDM System will not be routinely shared with external parties. The Wireless Service Provider generates and maintains data usage details for billing purposes, but that billing data is not part of any FTC

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
	Privacy Act or FISMA system except to the extent that such data is provided to the FTC and maintained by the FTC. Information transferred or shared outside the FTC's network will be secured in a manner consistent with FTC policies and procedures to reduce/minimize the risk of unauthorized disclosure of personal information. Such methods may include encryption of electronic information and hand delivery of documentation.
External Parties, Law Enforcement and/or Congress	Other than authorized personnel receiving MDM System or billing-related information to fulfill their job responsibilities (e.g., personnel responsible for managing any component of the MDM System) data generally will not be released to the Government, public, consultants, researchers, law enforcement, or other third parties. However, in the event the FTC receives lawful requests for the data from Congress or others, OCIO shall consult the HCMO, the OGC and/or the Privacy Office, as appropriate, with the goal of limiting the release of personally identifiable information. Whenever possible, aggregated, anonymous data will be provided using strategies designed to minimize the risk of re-identification. The FTC does not anticipate any routine sharing of personally identifiable information from the MDM System to outside entities. If such a request occurs, OCIO, HCMO, or OGC would track such disclosures to outside entities by documenting, among other things, which person or party/organization made the request, the date and nature of the request, the decision made to disclose or not disclose the data and by whom, any restrictions on further dissemination of the requested information, and the actual data disclosed.

3.2 Do contractors and/or third party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

OCIO contractors are authorized to access data in MDM to perform technical support relating to the operation of the system. The contractors are bound by non-disclosure agreements prohibiting unauthorized disclosure of information collected by the FTC. The contractors also are required to take the FTC's Security Awareness and Privacy Training course before being granted access to the FTC network, and annually thereafter to maintain access privileges.

MDM contractors do not generally access FTC data. However, in case of emergency where the FTC may be unable to access its own data and/or require continuity of operations services, MDM contractors have the ability to access FTC data and restore services as necessary.

3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third party service provider.

OCIO Contractors who access MDM are subject to the same rules and policies as FTC staff. They are also subject to the FTC's Breach Notification Response Plan.

MDM contractors abide by their internal incident response plan, which details steps to follow in case of a breach of federal agency information. In the event that FTC information is impacted, MDM contractors must notify the appropriate FTC official. All incidents involving data breaches, which involve PII, will be coordinated through the Privacy Office and the FTC's Breach Response Team.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

Users have no reasonable expectation of privacy while using FTC-issued Mobile Devices. Any business or personal communications or data transiting or stored on Mobile Devices may be used for any lawful purpose, and it may be intercepted, recorded, read, searched, seized, and disclosed by and to U.S. Government officials for official purposes.

☒ Notice is provided via (*check all that apply*):
- ☒ Privacy Act Statement (☒ Written ☐ Oral)
- ☐ FTC Website Privacy Policy
- ☐ Privacy Notice (e.g., on Social Media platforms)
- ☐ Login banner
- ☒ Other (*explain*): Mobile Device users are required to acknowledge their understanding of an agreement to comply with the above terms, and others, in the FTC Rules of Behavior, Privacy Act Statement, as well as the Annual Privacy and Security Awareness Training.

☐ Notice is not provided (explain): _____

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

When using an FTC-issued Mobile Device, individual users cannot decline to provide the information necessary for configuration, management, and administration of the Mobile Device.

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

Individual FTC employees and contractors (outside of authorized OCIO staff) do not have direct access to their own information in the MDM system. The individual user can contact the Help Desk and ask for assistance with gaining access to or requesting amendment/correction of MDM system information.

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

The individual user can contact the FTC Help Desk and request amendment/correction of MDM System information. The individual user can contact the help desk to register any complaints, concerns, or questions.

An individual may make a request under the Privacy Act for access to information maintained by the FTC about themselves in the Privacy Act systems maintained by the FTC. The FTC's privacy policy provides links to the FTC's SORNs, as well as information about making Freedom of Information Act (FOIA) requests and the online FOIA request form. Individuals must follow the FTC's Privacy Act rules and procedures, published in the Code of Federal Regulations (C.F.R.) at 16 C.F.R. 4.13. Access to information under the Privacy Act is subject to certain exemptions.

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

MDM

- The MDM contract obligates the vendor to maintain accurate, timely, and complete information.

Mobile Device

- Authorized FTC personnel routinely and automatically review information regarding Mobile Device configuration compliance (e.g., approved apps, applied security controls) by using MDM. The information stored on the Mobile Device by the user is not routinely or automatically reviewed by anyone other than the assigned Mobile Device user.

Mobile Device Billing Data

- FTC analysts review billing data monthly to ensure that the information is complete and accurate.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

MDM

- MDM information is protected from misuse and unauthorized access through various administrative, technical, and physical security measures. Technical security measures include limiting access to authorized individuals, requiring use of strong passwords, using encryption for certain data types and transfers, logging access, and regularly reviewing security procedures and best practices to enhance security. For example, MDM enforces a time-out function that requires users to re-authenticate after a specified period of inactivity so that unauthorized users cannot "piggyback" onto the credentials of a system administrator who forgot to sign out.

The FTC categorizes the information being exchanged between the MDM and the Mobile Devices as "moderate" using the Federal Information Processing Standards (FIPS) Publication 199, Security Categorization.[6] The FTC currently uses MaaS360 as its MDM solution. MaaS360 has a P-ATO issued by the FedRAMP Joint Authorization Board (JAB). The FTC will leverage the JAB P-ATO for MaaS360 when issuing the ATO for MDM.

Mobile Device

- Communication connections between the Mobile Device and FTC systems through MDM are encrypted. Additionally, each Mobile Device and SIM card is encrypted to prevent use on another device. MDM and the Mobile Device encryption mechanisms are validated in accordance with Federal Information Processing Standard (FIPS) 140-2. Additionally, each Mobile Device is encrypted with a passphrase. If supported by the Mobile Device, the user can choose to secure the Mobile Device with a fingerprint.

Mobile Device Billing Data

- The FTC HQ Data Center[7] provides security controls that protect billing data. FTC restricts access to billing data to authorized FTC employees and contractors on a least-privilege, need-to-know basis.

5.3 Has the system/project undergone the appropriate security risk assessment and received authority to operate?

The Mobile Device and Mobile billing data are part of the Datacenter GSS which underwent a risk assessment and received an Authorization to Operate on October 23, 2017. The current MDM solution underwent a risk assessment and received a FedRAMP Joint Authorization Board Provisional Authorization to Operate on August 5, 2015.

5.4 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

OCIO contractors are trained using the production data in MDM, which includes PII. The contractors are bound by non-disclosure agreements prohibiting unauthorized disclosure of information collected by the FTC. The contactors also are required to take the FTC's Security Awareness and Privacy Training course before being granted access to the FTC network, and annually thereafter to maintain access privileges.

MDM contractors do not use any FTC PII in the course of their system testing, training, or research.

[6] The potential impact of the loss of confidentiality, integrity, or availability is considered "moderate" if it is expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. The FTC relies on MDM and the Mobile Device security controls to secure sensitive FTC information, the loss or compromise of which could cause a significant degradation in mission capability. This includes potentially preventing the agency from being able to perform its primary functions, reducing the effectiveness of those functions, or result in significant damage to organizational assets or significant financial loss.

[7] The FTC Datacenter GSS is the primary IT infrastructure used by the FTC to host information systems that collect, process disseminate, and store information in support of the agency's mission. Refer to the FTC Datacenter PIA for details.

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

MDM

- MDM maintains an electronic profile of each authorized Mobile Device. The Mobile Device profile (See Section 2.1) is stored for as long as the user is authorized to access FTC systems via a Mobile Device and remains in possession of the Mobile Device.[8]
- MDM stores Mobile Device details and action history for auditing and reporting purposes (see Section 2.1). The action history is deleted from MDM by authorized FTC staff in accordance with NARA General Records Schedules (GRS). Mobile Device details are deleted when: (1) the Mobile Device is lost, stolen, or damaged and information on it must be wiped, or (2) the Mobile Device is no longer assigned to an employee.[9]

Mobile Device

- Application data resides on the Mobile Device until (1) deleted by the user, (2) deleted by services accessed by the mobile device such as those in the HQ Data Center policy, (3) deleted because Mobile Device is lost and wipe command is sent to Mobile Device, or (4) deleted because employee leaves the agency.
- When a Mobile Device is lost and cannot be promptly recovered after activating the geolocation function to determine current location, the Mobile Device will be wiped. When a Mobile Device is no longer required by an employee, the Help Desk deactivates the Mobile Device profile in MDM and wipes all information on the Mobile Device. The Mobile Device's SIM card is removed and destroyed in preparation for Mobile Device reuse by another employee.

Mobile Device Billing Data

- Billing data is kept electronically by the FTC in accordance with NARA GRS 1.1, Financial Management and Reporting Records.
- Monthly billing data is aggregated with previously collected billing information. The FTC retains aggregated billing data and disposes of the data in accordance with NARA GRS 1.1. Billing data on FTC backup media storage is deleted or over-written in accordance with FTC policy and procedures.

[8] Location data can be obtained by the FTC when an authorized system administrator activates the "Locate Device" function for an authorized purpose (e.g., Mobile Device is reported lost or stolen, Mobile Device is being billed at international roaming rates without prior notice, or otherwise as authorized or required by law.) MDMMDM does not retain geolocation data; however, geolocation data may be retained in the agency's electronic incident tracking system, Remedy, for up to five years.

[9] Geolocation data requested via MDM in not retained or stored by MDM but may be retained in the agency's electronic incident tracking system Remedy for up to 5 years.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

The MDM solution currently in use by the FTC is accessible through a Secure Hypertext Transfer Protocol (HTTPS) website. Authorized users must log in with their user IDs and passwords. The website uses session cookies to track user sessions in the web browser, and the cookies are encrypted with Secure Socket Layer (SSL)/Transport Layer Security (TLS) protection.

8 Privacy Risks and Evaluation

8.1 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

Risk	***Mitigation Strategy***
The system provides the capability to identify, locate, and monitor individuals.	The FTC does not use geolocation data to track or retain information about individual Device movement over time, and the FTC will not track Mobile Devices point to point or in real-time. Location data can be obtained by the FTC when an authorized system administrator activates the "Locate Device" function for an authorized purpose (e.g., if the Mobile Device is reported lost or stolen, if Mobile Device is being billed at international roaming rates without prior notice, or otherwise as authorized or required by law). As with all other MDM system information, the FTC limits review of location data in the system to authorized individuals for authorized need-to-know purposes. Billing data does not provide a capability to identify, locate, or monitor individuals in real-time, but it can reveal patterns of movement over time through numbers called and whether the Mobile Device used services nationally or internationally. The FTC will not use billing data except as described in this PIA.
Individuals who have access to PII could exceed their authority and use the data for unofficial/unauthorized purposes.	All Commission staff are subject to agency-wide policies and procedures for safeguarding PII and receive annual privacy and information security awareness training. Staff also receive additional, specialized role-based training focused on their specific position responsibilities. For example, HCMO staff receive additional training in the handling of employee information and IT administrators receive additional role-based training. Additionally, during the Mobile Device distribution and initial setup, users receive training on the security features and settings of their Mobile Device. Users are instructed to create strong passwords for the Mobile Device and are reminded to report any unexpected incidents pertaining to the Mobile Device to the Enterprise Service Desk.
Users could place sensitive personal information on the Mobile Device, which may expose the information to interception, storage, and sharing.	The FTC Rules of Behavior, policies, and training emphasize that the Mobile Devices are for official FTC use only. User activities and actions on the Mobile Devices may be seen, saved, and shared by the FTC and the U.S. Government for official purposes. This PIA makes no attempt to comprehensively record the types of non-FTC related data that users might choose to put on their FTC-issued Mobile Device; however, such data may

Risk	*Mitigation Strategy*
	include sensitive PII such as credit card numbers, contact information, photographs and videos, or data in the Mobile Device applications. Prior to receiving a Mobile Device, users are required to acknowledge that they understand the risk to personal information from using the Mobile Device for non-official purposes and that there is no reasonable expectation of privacy in any use of the Mobile Device. All FTC Mobile Devices are also encrypted to mitigate the risk of unauthorized access to information on the devices. Devices can also be remotely wiped if lost or stolen to prevent unauthorized access.
Reduced physical security controls may create greater risk of harm or loss.	The mobility of the Mobile Devices places them at higher risk of loss or theft than traditional IT resources. However, MDM enforces passphrase device encryption. MDM provides the ability to locate, lock and remotely erase a Mobile Device. Currently devices reported as lost are immediately locked and the information on the devices erased if not recovered within 24 hours. Devices reported as stolen are immediately wiped.
Individuals may potentially use untrusted or unsecured networks.	Mobile Devices can connect to non-FTC networks for Internet access and communication purposes, potentially exposing them to unprotected or unsecured wireless connections and other compromises. To decrease this risk, MDM enforces internet access through either the provided cellular network connection or an encrypted, password-protected network (preferably the employee's own controlled network). Additionally, transmissions between the Mobile Devices and MDM are encrypted at a level that comports with FIPS 140-2.
Individuals may potentially use applications or content created by unknown parties.	Personal use of FTC-issued Mobile Devices could increase the risk of malware infections from third-party applications. In addition, Mobile Devices with cameras may be subject to less obvious malware infection techniques, such as through Quick Response (QR) codes, which can be scanned by the Mobile Device's camera and might route the browser to malicious sites. User training emphasizes that the Mobile Devices are for official government use only, that applications should only be downloaded from the FTC app store for the Mobile Device, and that the user should contact the Help Desk if experiencing unexpected incidents pertaining to the Mobile Device. OCIO and the FTC Privacy Office conduct a security and privacy analysis of any applications that provided for download, and the Rules of Behavior remind users that the FTC has prohibited and prevented the installation of non-FTC-approved applications. OCIO can remove, "blacklist," or ban applications from the Mobile Devices. OCIO may periodically review the applications downloaded to check whether they pose an unacceptable risk to FTC information or systems. OCIO plans to route all web traffic for smartphones, similar to desktop computing, via the MTIPS internet path that includes URL filtering. This will ensure the browsing and security of smartphones matches that of all other computing environments at FTC.
Unauthorized disclosure or misuse of Mobile Device could result in substantial harm to the individual or organization.	Sharing Mobile Device data is permitted only if approved by HCMO, OGC and/or the Privacy Office, as appropriate.

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

The MDM Portal enforces a limit of five failed consecutive invalid login attempts by a user, regardless of the time elapsed between login attempts. The counter is only reset upon completion of a valid login.

FTC has configured a MDM session lock after 15 minutes of inactivity, after which time the pattern hiding functionality is inherited from the MDM provider.

The FTC has established four types of accounts that can access the MDM portal. These accounts are based on the role the individual is performing and the corresponding level of access needed in order to fulfill those duties. The four types of account are Auditor, Helpdesk Technician, Mobility Team Administrator, and the MDM Service Administrator.

1. The Auditor role has read-only permissions to view the current policy settings within the MDM portal. This role is provisioned to auditors and members of the CyberSec team, the FTC's security team.
2. The Helpdesk Technician role is assigned to all members of the Helpdesk team. This role has limited permissions and allows Helpdesk personnel to perform basic tier 1 support, such as locating or locking a mobile device.
3. The Mobility Team Administrator role is assigned only to members of the mobility team within Helpdesk support. This role has slightly more elevated privileges and allows members of the Mobility Team to set up new accounts and enroll Mobile Devices into the MDM application.
4. Lastly, the MDM Service Administrator is the account with super user privileges. This account has all the permissions necessary to manage FTC's instance of MDM, including establishing all of the device and security policy settings for the commission. This role is only granted by the System Owner to a limited number of individuals specifically tasked with administrating MDM on their behalf. The MDM service administrators monitor the use of MDM accounts on at least a monthly basis to ensure they are still valid and have not unjustly elevated their privileges beyond the scope of their assigned privileges. The account reviews are completed within the MDM portal utilizing pre-defined report queries that can be adjusted as needed. Additionally, whenever an account's permissions have been modified, an alert is automatically generated within MDM that is immediately displayed on the homepage of the MDM service administrators upon login, notifying them of the change.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).

The information is maintained and additional disclosures may be made in accordance with the applicable Privacy Act System of Records Notices – VII-3 Computer Systems User Identification and Access Records, VII-4 Call Detail Records, VII-7 Information Technology Service Ticket System, and VII-8 Administrative Service Call System. All of the FTC's SORNs are listed and can be downloaded from our public SORN page: http://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems.

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

Only authorized FTC staff have access to the MDM administrative console. The FTC has enabled the following events to be logged within the MDM portal:

- Successful / Unsuccessful account logon events
- Account management events
- Object access
- Policy change
- Privilege functions
- System events
- All Administrator activity
- Authentication checks
- Authorization checks
- Data deletions
- Data Access
- Data changes
- Permissions changes

The MDM Service Administrators reviews these logs on at least a monthly basis.

9 Approval and Signature Page

Prepared By:

_____ **Date: _____**
Jeffrey Smith
Office of Chief Information Officer (OCIO)

Reviewed By:

_____ **Date: _____**
John Krebs
Acting Chief Privacy Officer (CPO)

_____ **Date: _____**
Alexander C. Tang, Attorney
Office of the General Counsel (OGC)

_____ **Date: _____**
Jaime Vargas
Chief Information Security Officer (CISO)

_____ **Date: _____**
Yvonne K. Wilson
Records and Filing Office (RFO)

Approved By:

_____ **Date: _____**
Raghav Vajjhala
Chief Information Officer (CIO)