
**Federal Trade Commission**

**Privacy Impact Assessment**

**Mobile Device Management System**

**February 2015**

## 1. Overview

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: Mobility as a Service (MaaS) 360 is an externally hosted service used to centrally manage authorized FTC Mobile Devices and provide the following services:

- Secure Mail - provides encryption, compliant with Federal Information Processing Standards (FIPS) 140-2, for secure access to FTC email, calendar, and contact tools; an official government account is created for each authorized user that is specific to their Mobile Device
- Secure Browser - provides secure access to the FTC's intranet website and public websites
- Mobile Application Management - provides FTC-approved enterprise apps and disables the email and calendaring functions of the Mobile Device if the user attempts to install unauthorized apps

MaaS360 enforces security controls applied to the Mobile Device and notifies system administrators when a Mobile Device has fallen out of compliance. For example, all Mobile Devices are encrypted, and if a change in encryption status occurs, such as a user turning off encryption or removing and replacing SIM card, MaaS360 disables the Mobile Device and notifies the system administrator of the compliance issue.

Component 2: Mobile Devices are provided by the FTC to authorized users (currently, Mobile Devices are limited to either Apple iPhone or Samsung Galaxy devices). iOS-based devices provide 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.

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.

## 2. Data Collected and Stored Within the System

### 2.1 What information will be collected, used, disseminated or maintained in the system?

MaaS360

- User authentication credentials/user profile: employee name, user ID, FTC email address,

and password
- Mobile Device profile: Device ID, Mobile Device name, user name, Mobile Device type, manufacturer, model, operating system, International Mobile Equipment Identifier (IMEI/MEID, used to identify devices on the cellular network), installed date, last reported date, mailbox sync status, managed status(whether the mailbox has been appropriately synced), and MaaS360 enrollment status
- Authorized and unauthorized downloaded applications[1]
- Mobile Device location[2]
- 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 Device credentials: phone number, Mobile Device password, and user ID
- Active Directory Password – used to access MaaS360
- 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
- Browser - History/Usage data, which may indicate the user's preferences and can be collected by bookmarks, subscriptions to social media feeds, etc.
- FTC email, calendar, and contacts
- Downloaded documents received as email attachments
- Downloaded apps

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 the billing data shown below. The FTC does not use the CD[3], preferring to access the Provider's online portal. The CD is kept in a locked file cabinet for one (1) calendar year and is then disposed of by shredding. The following information is downloaded from the Mobile Device Service Provider and retained by the FTC and is the only billing data used by the FTC and covered by this PIA:

[1] 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] MaaS360 does not actively track Mobile Device location but can access current location information, if necessary and authorized. To view where a Mobile Device is located, an authorized administrator logs into the Maas360 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. See Section 6.3 for more information.
[3] To access the data on the CD requires that an application be installed on an FTC workstation; to avoid additional system administrative support, the FTC downloads the necessary data using the Provider's online portal.

- Mobile Device Telephone Number
- Employee Name
- Employee Organization
- 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)

## 2.2 What will be the sources of the information in the system?

MaaS360

- The system administrator creates a Mobile Device profile (See Section 2.1) 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.

Mobile Device

- Email, calendar, and contact information is synced to the Mobile Device via MaaS360 and the FTC's Outlook application.
- Documents are downloaded to the Mobile Device when the user opens email attachments.
- Authorized apps are acquired, installed, and updated via the MaaS360 App Catalog.[4]

Mobile Device Billing Data

- 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.

## 2.3 Why will the information be collected, used, disseminated or maintained?

MaaS360

- MaasS360 data is necessary for FTC IT staff to manage FTC Mobile Devices.
    - For example, MaaS360 allows staff to keep required applications up-to-date, reset passwords, and proactively secure the Mobile Devices.
    - Additionally, MaaS360 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

[4] Users who choose to download apps from the catalog of FTC-approved apps may choose to create and provide personal information that is stored on the Mobile Device, but users are not required to use any of the FTC-approved apps.

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 MaaS360 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 How will the information be collected?

MaaS360

- The information described in Section 2.1 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.

Mobile Device

- The information described in Section 2.1 is collected via initial configuration activities, as well as through routine daily use by the authorized user.

Mobile Device Billing Data

- The Wireless Service Provider makes electronic billing data available to the FTC.

### 2.5 Is the system using technologies in ways that the FTC has not previously employed (e.g., monitoring software)?

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

MaaS360

- Yes. MaaS360 is a new device management tool that combines existing functionality, software, and technologies that are common to the FTC's current infrastructure with new features such as the ability to locate Mobile Devices that are reported lost or stolen.

Mobile Device

- Yes. The Mobile Devices are currently limited to Apple iPhones and Samsung Galaxies and their associated functionality (e.g., use of FTC-approved apps) are new to the agency and are subject to the Limited Personal Use of Government Equipment policy, the FTC Mobile Device Rules of Behavior, and FTC ethics policies.

Mobile Device Billing Data

- No. The receipt, review, and retention of the billing data does not involve new technologies or data analysis methodologies.

**2.6. What specific legal authorities authorize the collection of the information?**

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

- Federal Information Security Management Act **(**44 U.S.C. 3541 *et seq.*)
- The FTC Act (15 U.S.C. §41 *et seq.*)
- The Commission's Rules of Practice
- 44 U.S.C. 3101 (records management by agency heads; general duties)

## 3. Data and Records Retention

**3.1 For what period of time will data collected by this system be maintained and in what form will the data be retained?**

MaaS360

- MaaS360 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.[6]

Mobile Device

[6] 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). If geolocation data is requested via MaaS360, MaaS360 will not retain that data; however, geolocation data may be retained in the agency's electronic incident tracking system Remedy for up to 5 years.

- Emails reside on the Mobile Device until (1) deleted by the user, (2) deleted by FTC Outlook policy, (3) deleted because Mobile Device is lost and wipe command is sent to Mobile Device, or (4) deleted because employee leaves the agency.
- Calendar information resides on the Mobile Device until (1) deleted by the user, (2) deleted because Mobile Device is lost and wipe command is sent to Mobile Device, or (3) deleted because the employee leaves the agency.
- Downloaded documents reside on the Mobile Device until (1) deleted by the user, (2) deleted because Mobile Device is lost and wipe command is sent to Mobile Device, or (3) deleted because employee leaves the agency.

Mobile Device Billing Data

- Billing data is kept electronically by the FTC in accordance with the FTC's NARA-approved comprehensive disposition schedule.

### 3.2 What are the plans for destruction and/or disposition of the information?

MaaS360

- MaaS360 stores Mobile Device details and action history (See Section 2.1) for auditing and reporting purposes. The action history is deleted from MaaS360 by authorized FTC staff in accordance with FTC's NARA-approved disposition schedule. Mobile Device details are deleted when: (1) the Mobile Device is lost, stolen, or damaged and must be wiped, or (2) the Mobile Device is no longer assigned to an employee.[7]

Mobile Device

- 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 MaaS360 and wipes 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

- Monthly billing data is aggregated with previously collected billing information. The FTC retains aggregated billing data, and authorized personnel dispose of the data in accordance with the FTC's NARA-approved disposition schedule. Billing data on FTC backup media storage is deleted or over-written in accordance with FTC policy and procedures.

## 4. Access to and Sharing of the Data

[7] Geolocation data requested via MaaS360 in not retained or stored by MaaS360 but may be retained in the agency's electronic incident tracking system Remedy for up to 5 years.

**4.1 Who will have access to the information in the system (internal and external parties), and with whom will the data be shared?**

MaaS360

- The FTC limits administrative access to MaaS360 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). MaaS360 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 personal activity, authorized FTC staff responsible for managing Mobile Devices may view the downloaded applications and personal 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.

- The FTC may also share the information in the MDM System in accordance with the applicable Privacy Act System of Records Notices. The FTC provides notice to employees of these possible disclosures, as discussed below in Section 5.1.

Mobile Device

- Authorized IT personnel may access information stored on a Mobile Device for authorized purposes. For example, Help Desk staff may access information on the Mobile Device 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 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 Inspector General (IG) for authorized purposes, as requested or required.

**4.2 If the data will be shared, how will the data be transferred or shared?**

In accordance with applicable Privacy Act System of Records Notices, MDM System component data necessary to configure, connect, and transmit data to the MaaS360

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 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.

**4.3 If the data will be released to the public, consultants, researchers or other third parties, will it be aggregated or otherwise de-identified (i.e. anonymized)? If yes, please also explain the steps that the Commission will take to aggregate or de-identify the data.**

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, as described in Section 4.1, 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.

**4.4 Do the recipients of the aggregated or de-identified information have another dataset, or is there a publicly available dataset that could be used to re-identify the information?**

The FTC does not expect to release MDM System data to the public, consultants, researchers, law enforcement, or other third parties. In the event such data needs to be released in response to a lawful request and may, consistent with that request, be released in modified form, the FTC to the greatest extent possible will use aggregation or de-identification strategies to limit the release of personal information and reduce/minimize the risk of re-identification of such information.

**4.5 Describe how the FTC will track disclosures of personally identifiable information that will be shared with outside entities.**

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.

**4.6 Do other systems share the information or have access to the information in this system? If yes, explain who will be responsible for protecting the privacy rights of the individuals affected by the interface (e.g., System Administrators, System Developers, System Managers)?**

No. The MDM System does not share information with other FTC systems.

## 5. Notice, Consent and Access for Individuals

**5.1 What notice will be provided to individuals about the collection, use, sharing and other processing of their personal data?**

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. 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, or later acknowledgements.

**5.2 What opportunities will exist for an individual to decline to provide information or to consent to particular uses of the information? If opportunities exist, how will this notice be given to the individual and how will an individual grant consent?**

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.

**5.3 What procedures will exist to allow individuals to gain access to their information and request amendment/correction, and how will individuals be notified of these procedures?**

The individual user can contact the Help Desk and ask for assistance with gaining access to or requesting amendment/correction of MDM System information.

## 6. Maintenance of Controls

**6.1 What controls will be in place to prevent the misuse of the information by those having authorized access and to prevent unauthorized access, use or disclosure of the information?**

<u>MaaS360</u>

- MaaS360 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 that are frequently changed, using encryption for certain data types and transfers, logging access, and regularly reviewing security procedures and best practices to enhance security. For example, MaaS360 has 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 MaaS360 and the Mobile Devices as "moderate" using the Federal Information Processing Standards (FIPS) Publication 199, Security Categorization.[8] The U.S. General Services Administration (GSA) has extended MaaS360 Authorization to Operate (ATO) in accordance with the U.S. Federal Information Security Management Act (FISMA).

Mobile Device

- Communication connections between the Mobile Device and FTC systems through MaaS360 are encrypted. Additionally, each Mobile Device and SIM card is encrypted to prevent use on another device. MaaS360 and the Mobile Device encryption mechanisms are validated in accordance with Federal Information Processing Standard (FIPS) 140-2. Additionally, each Mobile Device is protected by a strong passphrase that must be changed every 60 days. If supported by the Mobile Device, the user can choose to secure the Mobile Device with a fingerprint.

Mobile Device Billing Data

- The FTC network infrastructure 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.

**6.2 While the information is retained in the system, what will the requirements be for determining if the information is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?**

MaaS360

- The MaaS360 contract obligates the vendor to maintain accurate, timely, and complete information. The MaaS360 system will be audited and tested in accordance with FISMA

[8] The potential impact of the loss of confidentiality, integrity, or availability is considered "moderate" if it could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. FTC relies on MaaS360 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 to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; result in significant damage to organizational assets; or result in significant financial loss.

requirements to ensure vendor compliance.

Mobile Device

- Authorized FTC personnel routinely and automatically review information regarding Mobile Device configuration compliance (e.g., approved apps, applied security controls) by using MaaS360. 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.

**6.3 Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

MaaS360

- Yes. The FTC does not use GPS geolocation 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., 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). As with all other MaaS360 System information, the FTC limits review of location data in the System to authorized individuals for authorized need-to-know purposes.

Mobile Device

- Yes. The Mobile Device communicates directly with MaaS360, and the Mobile Device can be located, when authorized, as explained above.

Mobile Device Billing Data

- Yes. 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.

**6.4 Does this system comply with FISMA requirements to help ensure that information is appropriately secured?**

Yes, the MDM System (all components) meets all applicable FISMA requirements to ensure that information is appropriately secured.

**6.5 Describe the privacy training provided to users either generally or specifically relevant to the program or system.**

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.

## 7. Privacy Act

**7.1 Will the data in the system be retrieved by a personal identifier in the normal course of business? If yes, explain. If not, can it be retrieved by a personal identifier?**

MaaS360

- Yes, data in the MaaS360 may be retrieved using an employee's name, user ID, or email address.

Mobile Device

- All Mobile Devices are configured to be used by a specific employee using a specific user ID. Through routine daily use, data can be retrieved by personal identifier.

Mobile Device Billing Data

- Billing data may be retrieved by Mobile Device telephone number or Mobile Device identifier.

**7.2 Is the system covered by an existing Privacy Act System of Records Notice (SORN)? Provide the name of the system and its SORN number, if applicable.**

Yes. 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. Privacy Policy

### 8.1 Confirm that the collection, use and disclosure of the information in this system have been reviewed to ensure consistency with the FTC's Privacy Policy on www.FTC.gov.

The collection, use, and disclosure of the information in this system has been reviewed to ensure consistency with the FTC's Privacy Policy.

## 9. Privacy Risks and Mitigation

### 9.1 What privacy risks are associated with the collection, use, dissemination and maintenance of the data? How have those risks been mitigated?

The FTC strives to follow all NIST guidance and has implemented a risk-based approach to identify, assess, and prioritize risks associated with mobile computing, and determine the likelihood and potential impact of these risks. Mitigation strategies and resources are applied to defend against the most significant threats and reduce risk. The following are examples of FTC-identified privacy risks and the strategies employed to mitigate them:

- **Users placing 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 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.

- **Reduced physical security controls**. The mobility of the Mobile Devices places them at higher risk of loss or theft than traditional IT resources, which in turn subjects the data on them to increased risk of compromise. MaaS360 reduces this risk with controls that include encryption of data at rest and in transit, and the ability to locate and remotely erase a Mobile Device if it is lost or stolen.

- **Potential use of untrusted networks.** Mobile Devices can connect to non-FTC networks for Internet access and communication purposes, potentially exposing them to social engineering and other compromises. To decrease this risk, FTC recommends users use either the provided cellular network connection or an encrypted, password-protected network (preferably their own). Additionally, transmissions between the Mobile Devices and MaaS360 are encrypted at a level that comports with FIPS 140-2.

- **Potential use of 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 conducts a security analysis of any applications that it provides for business use, 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.

- **Unauthorized disclosure or misuse of Mobile Device data could result in substantial harm to the individual or organization**. As with all other MDM System information, the FTC limits access to Mobile Device location data from the MDM System to authorized individuals for authorized need-to-know purposes, and only collects location data when the "Locate Device" command is activated, as described in Section 6.3. Sharing Mobile Device data is permitted only if approved by HCMO, the OGC and/or the Privacy Office as appropriate and as described in Section 4.3.

**Appendix I – List of FTC-Approved Applications**

| Application Name | Distributed to all mobile devices | Distributed to specific groups of users[9] |
|---|---|---|
| Adobe Reader | **X** | |
| Maas360 Secure Browser | **X** | |
| Maas360 email | **X** | |
| Maas360 viewer/editor | **X** | |
| Google Maps | **X** | |
| Kayak | **X** | |
| Xe Currency | **X** | |
| Twitter | | **X** |

[9] Certain applications may be distributed to groups of users based on their user roles and business needs for such applications.

Prepared for the Business Owners of the System by:

_____ Date: _____
Jack F. Gabriel Jr.
Assistant Director Operations Assurance

Review:

_____ Date: _____
Alexander C. Tang, Attorney
Office of the General Counsel

_____ Date: _____
Katherine Race Brin
Chief Privacy Officer (Acting)

_____ Date: _____
Jeffrey Smith
Chief Information Security Officer

_____ Date:_____
Jeff Nakrin
Director, Records and Filings Office

Approved:

_____ Date:_____
Patricia Bak
Chief Information Officer (Acting)