Commodity Futures Trading Commission
Privacy Impact Assessment

System Name: Mobile Device Management (MDM) System

Office: Privacy

Date: February 4, 2014

1. Overview

The CFTC's mobile device management (MDM) system helps enable the CFTC workforce to securely access digital information and services anywhere, anytime, consistent with the **President's Digital Government Strategy (DGS)**. This system allows CFTC staff to conduct official government business while outside of the office, including making telephone calls, writing emails and using other forms of digital communication on CFTC-issued smartphones and tablets ("mobile devices"). The goals of MDM are to increase the methods by which employees can securely access CFTC systems; improve staff productivity by allowing staff to work on the devices that they know best and can use most efficiently; decrease wireless service costs; and provide additional control over sensitive CFTC information.

The MDM system is similar to the BlackBerry device management system (BlackBerry Enterprise System (BES)). The MDM will manage all CFTC non-BlackBerry mobile devices, giving the CFTC the ability to offer employees access to its information and systems on different types of mobile devices in a secure environment, and better ways to track data utilization rates and wireless service costs. Mobile device users will additionally have the same ability to search and look up colleagues from the Global Address List and contacts from their Outlook Email Contact Folders on their mobile devices as they do in front of their computers. Users can also access their Outlook calendars.

The privacy benefits of MDM include the technological separation of work information from employee personal data and/or applications that an employee may add to the device;[1] being able to authenticate all mobile devices connecting to CFTC systems; to remotely locate and delete data stored on a mobile device if it is lost, stolen or otherwise compromised; and the ability to ensure that the operating system and all of the CFTC applications running on the device are up-to-date. Another key privacy benefit is that MDM decreases the number of paper copies of CFTC information that employees use when they are outside the office. Instead, they can read, store and share digital copies of documents or other materials using mobile devices. The privacy risks and CFTC measures to mitigate those risks are discussed in Section 9 below.

The CFTC MDM system is comprised of three main elements:

[1] Note, however, that users have no reasonable expectation of privacy in their use of the CFTC-provided mobile device, as explained further in Section 2.1 and in the CFTC Interim Smartphone Rules of Behavior.

- the CFTC-issued mobile devices, including accounts for the application stores maintained by the creators of the device operating systems;
- the MDM platform, a web-based tool that manages the authenticated mobile devices, tracks usage data and applications downloaded to the device, etc., and which provides a dashboard of information for CFTC staff responsible for managing mobile devices. The current MDM platform is "MaaS360", which is short for "Mobile as a Service," **developed by Fiberlink, an IBM company**. The platform includes mandatory applications installed on the mobile devices, including:
    - calendar, contact information and email client;
    - secure browser;
    - remote desktop; (collectively, "the secure productivity suite" or "the required applications") and
- the **Wireless Expense and Asset Management System (WEAMS), provided by Verizon**.

Each component of the MDM system processes and stores unique types of information and uses different security and privacy protections designed to ensure confidentiality, integrity and availability of CFTC information, as explained below. CFTC staff who manage or oversee the MDM system or end-usage of devices will be granted access only to those components of the system that are relevant to their position descriptions after having demonstrated a "need to know" based on their official CFTC job responsibilities.

2. Data Collected and Stored Within the System

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

MaaS360 necessarily contains employee information to authenticate the user's mobile device to CFTC systems, e.g., employee name and device identifier. WEAMS contains data from CFTC-issued mobile devices for purposes of tracking data utilization, e.g., incoming and outgoing phone numbers, call length, cellular network usage, asset assignment by CFTC Division and billing details. This information is captured by the cellular network providers with which CFTC maintains a contract; the information is provided to CFTC staff responsible for managing mobile devices.

The information collected, used, disseminated and maintained in the MDM system for the mobile devices is generally the same type of information that is used to manage CFTC-issued BlackBerry devices. As shown in the table below, this can include applications downloaded to the device, calls made, photographs taken on the device, web sites visited, contact, email and calendar information, and content of communications and data transiting through CFTC systems or stored on the device.

Some information beyond that collected for the BlackBerry device system may be collected, used, disseminated and maintained in the MDM system due to different functionality available on different mobile devices, and also resulting from user downloaded or saved information. As to the latter, this PIA makes no attempt to record all of the types of information that users might place on the mobile devices, including content in personal email accounts, personal contacts, or data saved to the mobile device by personally-downloaded applications.

Just as with the BlackBerry devices and BES, users have no reasonable expectation of privacy on CFTC-issued mobile devices. Any business or personal communications or data transiting or stored on mobile devices may be used for any lawful purpose: 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 and agreement to comply with the above terms, and others, in the CFTC Interim Rules of Behavior Acknowledgment for CFTC-issued Smartphones or later acknowledgements.

1. PII Categories	2. Is collected, processed, disseminated, stored and/or accessed by this system or project	3. CFTC Employees	4. Members of the Public	5. Other (e.g. contractors, other government employees)
Name (for purposes other than contacting federal employees)	X	X	X*	X*
Date of Birth	X	X		
Full Social Security Number				
Tax Identification Number (TIN)				
Photographic Identifiers				
Driver's License				
Mother's Maiden Name				
Gender	**	**		
Mailing Address	X	X	X*	X*
Personal Email Address	X	X	X*	X*
Incoming and Outgoing Phone Numbers	X	X	X*	X*
Medical Records Number				
Medical Notes or some other Health Information				
Financial Account Information: credit card number	**	**		
Certificates				
Legal Documents				
Device Identifiers	X	X		
Web Uniform Resource Locator(s)	X	X		
Education Records				
Military Status				
Employment Status				
Foreign Activities				
Mobile device location information	X	X		

Other: any personal information added to the mobile device by the user, for example:	**X**	**X**		
Any applications downloaded by the user	**X**	**X**		
Any data saved to the mobile device by the downloaded applications	**X**	**X**		

*A reasonable user is likely to store the names, phone numbers, mail and email addresses of members of the public and/or contractors in the MDM system.
**During the account creation process for the application stores maintained by the creators of the device operating systems, mobile device users may be presented with the option to enter additional information, e.g., gender and credit card number. However, for the purposes of this PIA, it is assumed that a user will minimize these data types and not include a credit card number.

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

The CFTC user will generally provide or create the information collected by the MDM system through his or her use of the mobile device. Also, because these mobile devices access CFTC email and other systems, the sources of the information will include those sources of information in the CFTC systems, for example, individuals sending email to a user.

To download the required applications to the mobile devices, employees must create an account for the device manufacturer's application store. In addition, users must first unlock the mobile device and then log into the secure productivity suite to gain access to CFTC systems. The devices will capture the activity conducted on them.

The WEAMS tool will collect detailed call information and data usage reports on a monthly basis. This data will be generated by each of the wireless service providers with whom the CFTC enters into contracts.

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

The MDM system is designed to secure CFTC information and systems by allowing CFTC staff responsible for managing mobile devices to have granular control over them. For example, these staff will provision mobile devices, keep required applications up-to-date, reset forgotten passwords, and proactively secure the mobile devices. The MDM system will also allow these staff secure the devices by pushing operating system updates and security patches and helping ensure that employees use their CFTC-issued mobile devices securely and in accordance with CFTC privacy, security, limited personal use and confidentiality policies, procedures and memoranda.

In addition, WEAMS provides CFTC staff responsible for managing mobile devices tools to review and respond to the CFTC's changing data usage requirements and manage costs. The information collected by WEAMS will be used to analyze agency spending across multiple carriers resulting in cost reduction, proper invoicing, and optimization of wireless service contract agreements.

2.4. How will the information be collected by the Commission?

CFTC staff responsible for managing mobile devices create a profile for each CFTC employee assigned a mobile device that incorporates information from Windows Active Directory.[2] This information establishes that the employee is authorized to gain access to his or her calendar, contacts, email and remote desktop and will help ensure the accuracy of data usage information.

During the mobile device distribution and initial training, each employee will create an account for the device manufacturer's application store as well as at least one password that will allow him or her to download and access the required applications. Once the employee has signed the Interim Rules of Behavior and CFTC staff responsible for managing mobile devices have confirmed that the device is configured properly, the employee will be able to access the information described above.

The CFTC has entered into an arrangement for the WEAMS tool which allows the tool to collect data directly from certain wireless service providers. CFTC staff responsible for managing mobile devices will access the WEAMS tool and this information via a secure web portal. The web portal displays data usage and billing information in a sortable database, similar to a personal cellphone bill.

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

While the MDM system, its software and technologies, are common to the Commission's current infrastructure and consistent with the Commission's use of the BlackBerry device system, the enhanced functionality on the different mobile devices presents some differences. For example, the different mobile devices offer thousands of applications which users can easily download. These devices are government-issued, and must be used according to the Limited Personal Use policy and ethics rules. Yet, the CFTC cannot anticipate the applications that users could download to the device, nor can it anticipate the data that such applications could store on the device. Any such data could be accessed by the CFTC or other government officials for official purposes at any time, e.g., for servicing of the device, in response to a FOIA or congressional request, Inspector General or other investigation, or litigation.

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

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

- **5 U.S.C. 301** (Executive Department regulations);
- **41 CFR 101-35** (Telecommunications Management Policy); and
- **44 U.S.C. 3101** (Records management by agency heads; general duties).

3. Data and Records Retention

[2] Active Directory is a centralized database of CFTC network users and their levels of permission.

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

WEAMS maintains one year of detailed data usage information from the wireless service providers via the web portal. CFTC staff responsible for managing mobile devices will export the data from the web portal into spreadsheets to generate reports for the CFTC Chief Information Officer (CIO) and other staff with a need to know.

MaaS360 maintains a profile of each mobile device that is authorized to connect to CFTC systems (e.g. operating system, policy compliance state, device passcode status). The device's profile is stored within MaaS360 for as long as the user needs to access CFTC systems via a mobile device.

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

WEAMS stores one year of billing and data usage information. After that, the data is permanently purged from the web portal, and CFTC staff responsible for managing mobile devices also delete and/or destroy any saved copies of the information, except as may be required for litigation holds or other officials record-keeping requirements. These types of records are covered by **the National Archives and Records Administration General Records Schedule 12, item 2c**.

MaaS360 stores one year of device details and action history for auditing purposes. After that, the action history is permanently purged from MaaS360, and CFTC staff responsible for managing mobile devices also delete and/or destroy any saved copies of the information, except as may be required for litigation holds or other official record-keeping purposes. These types of records are covered by **the National Archives and Records Administration General Records Schedule 20, item 1c**. When an employee no longer requires a mobile device, ODT deactivates his or her device profile in MaaS360.

4. Access to and Sharing of the Data

4.1. Who will have access to the information in the system (internal and external parties), and with whom will the data be shared? If contractors, are the Federal Acquisition Regulations (FAR) clauses included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act)?

The CFTC restricts access to the WEAMS web portal to employees or contractors that are either staff responsible for managing mobile devices or are explicitly granted permission by their contracting officer. CFTC staff responsible for managing mobile devices will regularly provide the CIO with aggregated data usage rates and asset assignment information at the office or division level for review and forecasting purposes. The CIO may share this report with the Financial Management Branch (FMB) for budgeting purposes or others with a legitimate business need to know.

The CFTC similarly restricts access to MaaS360. CFTC staff or contractors who provide day-to-day operations and maintenance support, for example Customer Support Center staff and desktop administrators, will be allowed regular access to MaaS360 data stored in Fiberlink systems. These individuals need access to MaaS360 to respond to user questions, requests or incidents. MaaS360 automatically generates a report on the technical statuses of the mobile devices on a weekly basis and then emails that report to CFTC desktop administrators.

Additionally, the CFTC has the ability to conduct forensic analysis on any of the components of its systems, including the mobile devices and the MDM system. If a user installs personal applications or uses the mobile device for any personal activity, CFTC staff responsible for managing mobile devices may see the downloaded applications and personal activity. CFTC staff responsible for managing mobile devices may also be able to retrieve application usage, and the CFTC may disclose such usage in a Freedom of Information Act (FOIA), congressional or discovery requests or for other legitimate business purposes, for example, for CFTC Inspector General (IG) audits and/or investigations.

Just as with a CFTC desktop or laptop computer, any use of the mobile device could been seen, copied or stored by the CFTC. The CFTC may also share the information in the MDM system in accordance with the applicable Privacy Act System of Records Notices. The CFTC provides notice to employees of these possible disclosures, as discussed below in Section 5.1.

CFTC contractors with access to the MDM system, including information security specialists, are required to comply with the Privacy Act and CFTC information usage policies and procedures contractually through either FAR terms or other terms and conditions.

4.2. If the data will be shared outside the Commission's network, how will the data be transferred or shared?

MDM system data will not be shared outside of the Commission's network, except with the Fiberlink systems that store MaaS360 data, and in accordance with applicable System of Records Notices. (Note that the wireless service providers themselves generate and maintain data usage details for billing purposes; this data feeds into the MDM system.) If transferred or shared outside the Commission's network, the data will be transferred in a manner consistent with CFTC policies, procedures and memoranda and designed to prevent the unauthorized disclosure of sensitive information. Such methods may include encryption of electronic information or 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 contractors receiving MDM information to fulfill their job responsibilities, e.g., contactors responsible for managing mobile devices, MDM system data generally will not be released to the public, consultants, researchers or other third parties.

However, as described in Section 4.1, in the event that the CFTC receives lawful requests for the data from Congress or others, ODT shall consult the Human Resources Branch (HRB), the Office of General Counsel (OGC) and/or the Privacy Office, as appropriate, with the goal of minimizing any release of identifiable information, and whenever possible, providing aggregated, anonymous data using strategies designed to prevent re-identification through other available information.

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 Commission information?

As explained above, other than certain contractors, the CFTC does not expect to release MDM system data to the public, consultants, researchers or third parties. In the event such data needs to be released through a lawful request and may be released in aggregated form, the CFTC to the greatest extent possible will use aggregation or de-identification strategies designed to prevent re-identification of such information through other available information. The CFTC recognizes that certain CFTC employee information is publicly available on the internet.

4.5. Describe how the CFTC will track disclosures of personally identifiable information that will be shared with outside entities. The Privacy Act requires that the CFTC record the date, nature, and purpose of each disclosure of a record to any person or to another agency.

Although any disclosure in PII-form outside the CFTC is unlikely, ODT, HRB 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, and any restrictions on further dissemination of the requested information.

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 CFTC 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?

Following is the Privacy Act Notice for the MDM system which is included in the CFTC Interim Rules of Behavior Acknowledgment for CFTC-issued Smartphones:

> The collection of data for the CFTC's mobile device management system is authorized by 5 U.S.C. 301, 41 CFR 101-35 and 44 U.S.C. 3101. The primary use of this information is to facilitate secure access to CFTC systems when outside the office, so that employees can make phone calls and use other forms of digital communication to complete their official work assignments. This information will be regularly analyzed by the Office of Data and Technology (ODT) and may be shared with your supervisor, other managers in your chain of command, and the CFTC Human Resources and Financial Management Branches. To the extent this information indicates a possible violation of civil or criminal law, it may be shared with an appropriate Federal, state or local law enforcement agency. The information will be maintained and additional disclosures may be made in accordance with the applicable Privacy Act System of Records Notices. You are not required by law to provide the information requested, but if you do not provide it the CFTC will not be able to make a mobile device available to you.

The warning banner appearing when a user logs into CFTC systems applies to the MDM system:

> This is a United States Government information system operated by the Commodity Futures Trading Commission ("CFTC"). The information system may be accessed and used only for official Government business and other authorized use by authorized personnel. The information system includes computers, computer networks, and all equipment, devices and data storage media attached to the CFTC network or to a computer on such network provided by the CFTC. Unauthorized access or use of this information system is prohibited and may subject violators to criminal, civil, and/or administrative action. Any communications or data transiting or stored on this information system may be used for any lawful Government purpose. You have no reasonable expectation of privacy in any communication or data transiting or stored on this information system; all information transiting or stored in this information system may be intercepted, recorded, read, copied, searched, seized and disclosed by and to authorized personnel for official purposes consistent with CFTC policies. The Government routinely intercepts and monitors communications and information on this information system, for example, to address security vulnerabilities and other risks.
>
> Note that this notice supersedes any other log-in banner that may appear on other CFTC issued equipment, including CFTC-issued laptops.
>
> By using this information system, whether authorized or unauthorized, or by clicking "OK" below, you acknowledge that you have read, understand and consent to the above.

The CFTC Interim Rules of Behavior Acknowledgment for CFTC-issued Smartphones also explain that users shall have no reasonable expectation of privacy with regard to any business or personal communications or data transiting or stored on the mobile device.

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?

The MDM system is mandatory for all mobile devices that connect to CFTC systems so that CFTC can manage such devices and control data usage costs. If a staff member prefers not to use a mobile device to connect to CFTC systems, the staff member should speak with his or her supervisor.

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?

As to phone and data usage and as described in the CFTC Interim Rules of Behavior Acknowledgment for CFTC-issued Smartphones, employees may be liable for charges for fees in excess of the mobile device's data plan. CFTC staff responsible for managing mobile devices review all wireless bills on a monthly basis to ensure billing accuracy and to address possible errors and abuse. CFTC staff responsible for managing mobile devices, FMB or HRB will notify the mobile device user about any billing-related concerns should they arise. CFTC staff responsible for managing mobile devices, FMB or HRB will also provide a user the opportunity to review his or her data usage

information and to explain or dispute any potential overages or inaccuracies. If a user has questions about his or her data plan, he or she should consult the Telecommunications group in ODT or appropriate Business Manager**.**

Contact the Privacy Team or the Office of General Counsel General Law Division to request access to other types of data that may be stored by the MDM system.

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?

MDM system information is protected from misuse and unauthorized access through various administrative, technical and physical security measures. For example, physical measures restrict building access to authorized individuals only.

Technical security measures include restrictions on computer access to authorized individuals, required use of strong passwords that are frequently changed, use of encryption for certain data types and transfers, and regular review of security procedures and best practices to enhance security. For example, both WEAMS and MaaS360 have a time-out function that requires users to re-authenticate after a specified period of inactivity so that unauthorized users cannot "piggyback" on the credentials of a user who forgot to sign out.

Access to the WEAMS web portal will be restricted to employees or contractors that are either responsible for managing mobile devices or individuals with explicit permission granted by the contracting officer or CFTC staff responsible for managing mobile devices. Individuals who wish to gain access to WEAMS information must be granted credentials for use including a unique user ID and password. In addition, accounts are based on roles and permissions that limit visibility into the system, allowing staff only to have access to relevant information as defined by their business needs.

The CFTC categorizes the information being exchanged between MaaS360 and the mobile devices as "moderate" under the **National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 199 Security Categorization**.[3] According to Fiberlink, **MaaS360 has an authority to operate** (ATO) in accordance with the U.S. Federal Information Security Management Act (FISMA) by the U.S. General Services Administration (GSA).

Connections between the mobile devices and CFTC systems through MaaS360 are encrypted. Additionally, each mobile device is encrypted. **WEAMS** and **MaaS360** encryption mechanisms are validated in accordance with Federal Information Processing Standard (FIPS) 140-2.

[3] 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. CFTC relies on MaaS360 to secure sensitive CFTC 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.

Both the mobile device and/or the contents of the secure productivity suite can be completely erased in the event that the mobile device is lost, stolen or otherwise compromised. Finally, audit logs are generated by both MaaS360 and WEAMS and are reviewed by CFTC staff responsible for managing mobile devices when they encounter any abnormal conditions.

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?

The data collected within WEAMS will consist of detailed calling records, minutes and data utilization by device, wireless service provider cost breakdown, and asset assignment by CFTC division. In the past, CFTC staff responsible for managing mobile devices reviewed these records in a more manual process. WEAMS centralizes the data so that it is easier to track and verify. In addition, the CFTC will continue to receive paper bills from its contracted wireless service providers to allow it to crosscheck the accuracy of data displayed in WEAMS.

As to the data that may be stored in MaaS360, the CFTC has a contract with Fiberlink which obligates Fiberlink to maintain accurate, timely and complete information. CFTC staff responsible for managing mobile devices will periodically check the status of mobile devices in MaaS360 to verify that the retained information meets the requirements of the contract. MaaS360 will also be tested and audited regularly, in accordance with FISMA requirements.

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

To protect the mobile device and CFTC information accessible through the device, the MDM system allows CFTC to determine the general location of the mobile devices at designated intervals. Mobile device location data may be sensitive PII because, if it is lost, compromised, or disclosed without authorization, it could result in substantial harm to an individual. For example, for call billing purposes, the WEAMS tool keeps a record of the general location of the mobile device when calls are placed or received. As with all other MDM system information, the CFTC limits access to location data accessible through the MDM system strictly to those with a need-to-know (please see the CFTC's policy on Safeguarding Personally Identifiable Information for additional details).

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

Yes. According to the developers of MaaS360 and WEAMS, those components adhere to 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.

Commission staff are subject to agency-wide policies and procedures for safeguarding PII and receive annual privacy and security training. Many staff receive additional training focused on their specific job duties. For example, HRB staff receive additional training in the handling of employee information, and ODT domain 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 learn how to create strong passwords for the device and secure productivity suite and are reminded to report any unexpected incidents pertaining to the mobile device to the DC or regional ODT Support Center immediately.

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?

Yes, data in MaaS360 may be retrieved using an employee's name or employee ID number. In WEAMS, data may be retrieved by the employee's mobile device telephone number or 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.

The Privacy team is updating CFTC-34, Telecommunications Services to include the MDM system.

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 CFTC's Privacy Policy on **www.cftc.gov**.

The CFTC's Privacy Policy on **www.cftc.gov** is not applicable to the mobile device management system. As mentioned above in Section 5, information concerning the collection, use and disclosure of this information is available to employees on the Privacy Office's CFTCnet website.

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?

Mobile devices face some of the same privacy threats as desktop computers. However, these devices are subject to additional unique threats because of their size, portability, always-on wireless connections, physical sensors (e.g., camera, microphone) and location services (e.g., triangulation of the phone location by cell towers to determine phone location, Global Positioning System). The diversity of available devices, operating systems, carrier-provided services (e.g., Short Message Service, browser, email), and mobile applications present privacy challenges not only for CFTC information, but also personal information. Depending upon which services are implemented or activated, these additional threats can increase the device's vulnerability to interception or alteration of communications and the risk to personal privacy.

These threats are constantly changing and the CFTC addresses them as mobile technology evolves. The mitigation strategies that the CFTC employs to reduce the risks associated with these threats involve applying management, operational and technical controls to each element of the mobile architecture. Management controls include

educating users about personal privacy risks and how they can minimize such risks, and offering privacy and security awareness training to address mobile device-specific threats and to reinforce policies defining Rules of Behavior and Limited Personal Use of mobile devices.

The CFTC strives to follow all NIST guidance and implement 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 then applied to defend against the most significant threats and reduce risk. The following are examples of CFTC-identified privacy risks accompanied by the strategies that ODT, the Telecommunications group and the Privacy Team are employing to mitigate them:

- **Users could place any type of sensitive personal information on the mobile devices, exposing such information to interception, storage and sharing**: In its Rules of Behavior, policies and training, CFTC has emphasized to users that the devices are for official CFTC business only. Anything that users do with the mobile devices may be seen, saved and shared by the CFTC and the U.S. Government for official purposes. This PIA makes no attempt to comprehensively record the types of data that users might put on the mobile devices, however such data may include sensitive PII like credit card numbers, contact information, photographs and videos, or data in personal applications. Prior to receiving a mobile device, users are required to acknowledge that they understand the risk to personal information from using the device for non-official purposes and that there is no reasonable expectation of privacy in any use of the mobile device.
- **A lack of physical security controls**: The mobility of the 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 counters this risk by encrypting data in storage and transit and enabling CFTC staff responsible for managing mobile devices to locate and remotely erase the devices if they are lost or stolen.
- **Use of untrusted networks**: Mobile devices can connect to non-CFTC networks for internet access and communication purposes, potentially exposing them to eavesdroppers. To decrease this risk, CFTC instructs users to 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.
- **Use of applications or content created by unknown parties**: Personal use of CFTC-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 device's camera and then route the browser to malicious sites. User training emphasizes that the mobile devices are for official government use only and to contact the Customer Support Center should the user experience any unexpected incidents pertaining to the mobile device. ODT conducts a security analysis of any applications that it provides for business use. Also, if ODT becomes aware of a significant vulnerability in an application that users have downloaded, it will remove and "blacklist" or ban that application from the mobile devices. ODT may periodically review the applications downloaded to check whether they may pose an unacceptable risk to CFTC information or systems.
- **Mobile device location data may be sensitive PII because its unauthorized disclosure or misuse could result in substantial harm**: As with all other MDM

system information, the CFTC limits access to location data accessible through the MDM system strictly to those with a need-to-know. The CFTC is committed to providing a safe and secure work environment. Sharing mobile device data is permitted only if approved by HRB, the OGC and/or the Privacy Office as appropriate and as described in Sections 4.1 and 4.2, for example in order to allow FMB to analyze data usage rates and to create budgets, or for the IG to conduct audits and investigations.