Commodity Futures Trading Commission
Privacy Impact Assessment

System Name: Mobile Device Management (MDM) System

Office: Office of Data and Technolgy (ODT)

Date: March 1, 2019

1. Overview

The CFTC's Mobile Device Management (MDM) system is a software solution that is installed on CFTC-issued smartphones and tablets ("mobile devices") and enables the CFTC staff to securely access CFTC information and services to conduct official government business. 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 solution allows the CFTC Office of Data and Technology (ODT) to centrally manage and administer CFTC issued mobile devices. This includes: authenticating mobile devices to connect to internal CFTC systems; remotely deleting data stored on a mobile device if it is lost, stolen or otherwise compromised; and ensuring the operating system and all of the CFTC applications running on the device are up-to-date.

The current MDM platform is "MaaS360", which is short for "Mobile as a Service," developed by Fiberlink, an IBM company. The platform requires mandatory applications installed on the mobile devices including:

- Email client
- Calendar
- Contact information
- Secure browser
- Remote desktop

Devices are managed using a web portal that is hosted externally by the MDM solution provider. Access to the web portal is restricted to CFTC staff that have a need to know the information to manage and oversee the mobile devices.

2. Data Collected and Stored Within the System

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

This PIA covers the personal information collected and maintained by the MDM application to enable CFTC-issued devices to connect to CFTC systems and allow users to access and use the information. The PIA does not cover all of the categories of

personal information a user may have access to, or interact with, such as email content that resides and is managed on internal CFTC systems.

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	**X**	**X**		**X***
Date of Birth				
Full Social Security Number				
Tax Identification Number (TIN)				
Photographic Identifiers				
Driver's License				
Mother's Maiden Name				
Gender				
Mailing Address				
Email Address	**X**	**X**		**X**
Phone Numbers				
Medical Records Number				
Medical Notes or some other Health Information				
Financial Account Information: credit card number				
Certificates				
Legal Documents				
Device Identifiers	**X**	**X**		**X**
Web Uniform Resource Locator(s)	**X**	**X**		**X**
Education Records				
Military Status				
Employment Status				
Foreign Activities				

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

The information is collected directly from the user. This includes information collected during the mobile device registration process, and from the mobile device itself as it is used.

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

The information is collected to enable the CFTC Office of Data and Technology (ODT) staff to manage CFTC mobile devices. MDM allows staff to keep required applications up-to-date, reset passwords, and proactively secure the mobile devices.

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

The 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.[1] This information establishes that the employee is authorized to gain access to his or her calendar, contacts, email and remote desktop and helps ensure the accuracy of data usage information. In addition, during the mobile device distribution and initial set up, each employee will create an account for the device manufacturer's application store.

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

No. The system is not using technologies in ways that the CFTC has not previously employed. The system does not have geolocation tracking enabled to monitor or physically track an individual.

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

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

- 41 CFR 101-35 (Telecommunications Management Policy);
- 44 U.S.C. § 3551 et seq. (Federal Information Security Modernization Act),
- 5 U.S.C. 301 (Executive Department regulations); and
- 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 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). Data collected by the device will be maintained for one year based on the date created.

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

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 3.2, item 030. 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

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

Acquisition Regulations (FAR) clauses included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act)?

CFTC staff or contractors who provide day-to-day operations and maintenance support, for example Customer Support Center staff and desktop administrators, may be allowed access to MaaS360 data stored in the system. These individuals need access to MaaS360 to respond to user questions, requests, or incidents. MaaS360 automatically generates a report on the technical status of the mobile devices and this is emailed to CFTC desktop administrators.

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.

The CFTC may also share the information in the MDM system in accordance with the applicable Privacy Act System of Records Notice. 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 are required to comply with the Privacy Act and CFTC information 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 vendor that stores MaaS360 data, and in accordance with applicable System of Records Notice.

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., contractors responsible for managing mobile devices, MDM system data ordinarily will not be released to the public, consultants, researchers or other third parties, however, the agency may be required to do so under a legal demand (e.g. subpoena, FOIA request, Congressional inquiry).

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?

The CFTC does not expect to release MDM system data to the public, consultants, researchers, or third parties.

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, CFTC is able to track the disclosure of information back through the original request.

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)?

The MDM system shares information with internal CFTC systems to be able to authenticate the individual using the device to access internal CFTC information. System Administrators are responsible for ensuring privacy is properly protected in these 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?

This PIA and the SORN included in section 7 below provide notice regarding the collection, use and sharing of personal data.

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. A CFTC staff member can decline to provide information, but this will exclude them from receiving and using a CFTC 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?

A CFTC staff member can contact the Office of Data and Technology if they are having issues with their mobile device. An individual may also follow the process outlined at CFTC.gov/privacy and 17 CFR 146.8 to file a Privacy Act request.

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 safeguards. Administrative safeguards include agency-wide Rules of Behavior, procedures for safeguarding personally identifiable information, and required annual privacy and security training.

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. MaaS360 has 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. Connections between the mobile devices and CFTC systems through MaaS360 are encrypted, and each mobile device is encrypted.

In addition, 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 MaaS360 and reviewed by CFTC staff responsible for managing mobile devices when they encounter any abnormal conditions.

Physical security measures include restrictions on building access to authorized individuals, access controlled server space, and maintenance of records in lockable offices and filing cabinets.

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 is upgraded, tested, and audited regularly to ensure the system is functioning properly and operating as intended. Inaccurate or outdated information is evaluated as part of this process.

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

No. The MDM system has the ability to remotely wipe data from the device, but the geo-location tracking functionality is not enabled in the system.

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

Yes. MaaS360 is a FedRAMP authorized product and complies with 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.

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 is retrieved using an employee’s name or employee ID, 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.

Yes. CFTC-35, General Information Technology records covers the mobile device management system records.

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. CFTC addresses mobile devices in a number of internal policies and procedures that address using Government systems and information.

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 risks as desktop computers. However, these devices are subject to additional risk 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 mitigation strategies that the CFTC employs to reduce these risks 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; offering privacy and security awareness training to address mobile device-specific threats; implementing mobile device specific policies and procedures including IT Rules of Behavior and limited personal use requirements.

The CFTC follows NIST guidance and implements a risk-based approach to identify, assess, and prioritize risks associated with mobile computing, and to 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. 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 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 with Federal Information processing Standard (FIPS) 140-2 level encryption.
- **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. 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 behavior 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.