Privacy Impact Assessment
for
Microsoft 365 (M365)

November 09, 2021

System/Business Owner

Dev: Juned Shaikh; O&M: William Yuen

Reviewing Official
Charles Cutshall
Chief Privacy Officer
Commodity Futures Trading Commission

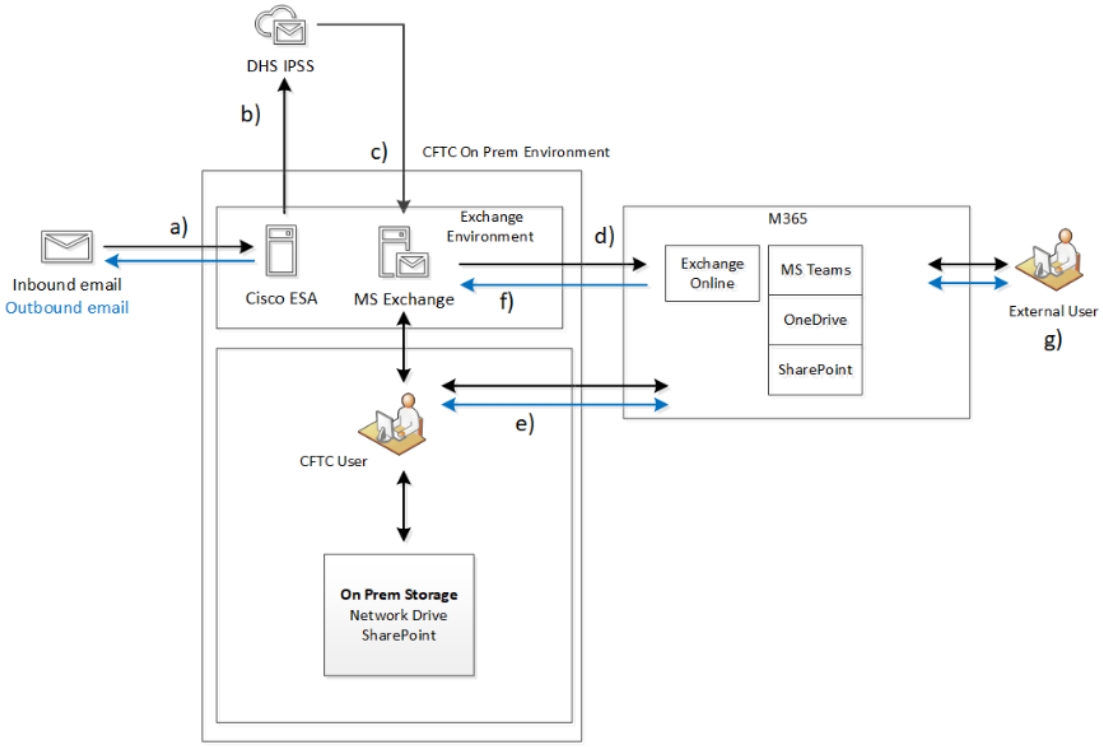
I. SYSTEM OVERVIEW

1) Describe the purpose of the system/collection:

Microsoft 365 (M365) is a Software-as-a-Service (SaaS) product from Microsoft that includes Microsoft's Office Productivity Suite with online versions of Microsoft's communications and collaboration services. M365 will allow the CFTC to simplify administration of licenses and subscriptions to services at an enterprise level and facilitate system-wide user management, password administration, and oversight of security and privacy controls. Information collected, maintained, used, or disseminated by M365 includes end-user contact information, email messages (including any attachments), Teams standard and private channel conversations and posts, Teams chat messages, files, wiki, calendars, meetings, tasks, and audit log information. End-users of the system are limited to CFTC staff that includes employees, contractors and interns, but M365 also captures information about non-CFTC individuals if non-CFTC individuals communicate or collaborate with a CFTC user. The CFTC is not opening Teams to guest users, so non-CFTC individuals cannot participate in Teams chat or channel conversations. However, non-CFTC individuals may participate in Teams meetings and will be captured on meeting recordings stored in Teams. The CFTC is currently in its first phase of deploying M365. Initially, the CFTC will deploy a hybrid email solution running both an on-premises Exchange environment and M365 Exchange Online.

This privacy impact assessment (PIA) evaluates the privacy implications for CFTC's use of the M365 Teams application including OneDrive, and Teams SharePoint sites, and Exchange Online. This PIA will be updated to address additional privacy risk as other service products are implemented.

2) Provide a data map or model illustrating how information is structured or is processed by the system throughout its life cycle. Include a brief description of the data flows.



a) Incoming email is scanned for threats by Cisco's Email Security Appliance (ESA) located within CFTC's network boundary.
b) Email is routed to and scanned by the Cybersecurity and Infrastructure Security Agency's (CISA) intrusion prevention protection security system (IPSS). Read more about the EINSTEIN IPSS system at: https://www.cisa.gov/einstein
c) Email which is cleared by the DHS IPSS reaches the Exchange server within the CFTC's network boundary.
d) A copy of the email is sent from the on premises (a.k.a., on prem) Exchange server to Exchange Online.
e) CFTC staff receive and send email using their Outlook mailbox(es) that are connected to their Exchange account(s).
f) Outgoing mail follows the same route from the Exchange Server to ESA, except that outgoing email is not scanned by the DHS IPSS.
g) Using MS Teams, CFTC staff are able to send and receive standard and private channel conversations and posts, chat messages, files, wiki, calendars, meetings, tasks, and audit log information, as well as host video conferences and store recordings of meetings with external users, but cannot transfer files to or receive files from external users at this time.

II. AUTHORITY AND PURPOSE

1) What is the legal authority to collect, use, maintain, and share information in the system?

7 U.S.C. 1 *et seq.*, including Section 12 of the Commodity Exchange Act, at 7 U.S.C. 16, and the rules and regulations promulgated thereunder. See also 7 U.S.C. 22(a)(2)-(3).

III. INFORMATION TYPES

1) What information will be collected, maintained, used, and/or disseminated?

Due to the nature of M365, all types of PII could potentially be collected, maintained, used, and/or disseminated using M365.

Identifying Numbers	
☒ Social Security Number	☒ Truncated or Partial Social Security Number
☒ Driver's License Number	☒ License Plate Number
☒ Patient ID Number	☒ File/Case ID Number
☒ Student ID Number	☒ Health Plan Beneficiary Number
☒ Passport Number	☐ Federal Student Aid Number
☒ Employee Identification Number	☒ Taxpayer Identification Number
☒ Professional License Number	☒ Legal Entity Identifier
☒ Credit/Debit Card Number	☒ National Futures Association ID
☒ Personal Bank Account Number	☒ Other ID if it can be traced back to an individual
☐ Personal Device Identifiers or Serial Numbers	
Contact Information	
☒ Personal Mobile Number	☒ Business Phone Number
☒ Personal E-mail Address	☒ Business E-mail Address
☒ Home Phone Number	☒ Personal or Business Fax Number
☒ Home Mailing Address	☒ Business Mailing Address
Sole Proprietors	
☒ Business Taxpayer Identification Number	☒ Business Mailing Address
☒ Business Credit Card Number	☒ Business Phone or Fax Number
☒ Business Bank Account Number	☒ Business Mobile Numbers
☒ Business Device identifiers or Serial Numbers	☒ Business Email
Biographical Information	
☒ Name	☒ Gender
☒ Date of Birth	☒ City or County of Birth
☒ Country of Birth	☒ Zip Code
☒ Citizenship	☒ Military Service Information
☒ Spouse Information	☒ Academic Transcript
☒ Group/Org. Membership	☒ Resume or Curriculum Vitae

☒ Location Data (e.g., GPS)	☒ Nationality
☒ Employment Information	☒ Marital Status
☒ Mother's Maiden Name	☒ Children Information
Biometrics/Distinguishing Features/Characteristics	
☐ Fingerprints	☐ Height
☐ Retina/Iris Scans	☒ Voice/Audio Recording
☐ Hair Color	☐ Eye Color
☒ Video Recording	☒ Photos
☐ Weight	☒ Signatures

2) What information relating to users of the M365 solution will be collected, maintained, used, and/or disseminated?

Active Directory/Device Information	
☒ IP Address	☒ MAC Address
☒ CFTC Asset Number	☒ Device Identifiers or Serial Numbers
☒ User Name / Password	☒ Log data

IV. COLLECTING INFORMATION

1) How is the information in this system collected?

Information is collected and stored in M365 when an account is created and when the account is used to create documents using MS Office applications, and to send and receive email, Teams standard and private channel conversations and posts, Teams chat messages, files, wiki, calendars, meetings, tasks, and audit log information. The information collected includes the content of email messages, attachments, Teams conversations and messages, Office files, and metadata such as the email address and message log information (such as internet protocol (IP) address, date of message, and time of message).

2) If any forms are used to collect information that resides in the system, please include the name of such form(s) and any applicable control number (i.e. issued by CFTC, OMB, etc.).

No forms are used to collect information that resides in the system, aside from completed forms that may be stored in M365 as email attachments, or other MS Office documents.

V. INFORMATION USE

1) Will information in the system be retrieved using one or more of the data elements listed in Section III?

   CFTC end-users can use the search feature in Outlook and Teams to retrieve information by CFTC end-user name and can retrieve other information (such as information contained in email messages and instant messenger/IMs) by name or other identifiers using a full-text search capability. System administrators can retrieve CFTC end-user account information and audit log information by end-user name or other end-user identifiers.

2) If the information in the system is retrieved using one or more of the identifiers, what CFTC System of Records Notice (SORN) covers the information?

   Depending on the content and how it is retrieved, information maintained in M365 may be covered by a number of CFTC SORNs. Links to all published CFTC SORNs are available at: https://www.cftc.gov/Privacy/SORN/index.htm

VI. ACCESS AND SHARING

1) With which internal CFTC Offices or Divisions is the information shared? For each Office or Division, what information is shared and for what purpose?

   M365 is intended to be an agency-wide tool to facilitate the collaboration and sharing of information. Therefore, emails and IMs may be sent between the different CFTC Offices and Divisions to perform their mission activities. Access to M365 is restricted to authorized CFTC end users who must adhere to the CFTC Rules of Behavior, the Privacy Act of 1974, and other laws, regulations, CFTC policies, and guidelines pertaining to the appropriate use and disclosure of PII.

2) Approximately how many users have access to the system?

   Approximately 1,100 users will have access to the system.

3) How is the information shared internally?

   Information in M365 is shared internally using email or Teams IMs and video conference functionality. Sharing of log data is described in the CFTC's Splunk PIA, available at: https://www.cftc.gov/Privacy/cftcpia/index.htm

4) With which external organization(s) is the information shared?

CFTC staff in the proper course of their duties may share information by email, or by video conference with other Federal agencies, public and private entities, as well as individual members of the public.

5) How is the information shared externally?

Information is shared externally by any necessary or convenient media.

VII. TRANSPARENCY

1) How are individuals notified as to how their information will be collected, used, and/or shared within this system?

To provide transparency and allow CFTC users to understand how their communications and other information will be handled, a warning banner is displayed on the login screen that CFTC end-users see when they log in to their workstations. This banner informs users that any information they transmit through the CFTC network device may be monitored, intercepted, searched, and/or seized by the Commission.

To the extent that M365 collects and maintains information protected by the Privacy Act pertaining to non-CFTC staff, notice that the Commission is capturing the information is further provided by (i) this PIA, (ii) the Commission's website privacy policy, which specifies the collection and use of personal information users voluntarily provide to the Commission, and (iii) the Commission's SORNs. To the extent information is collected through other systems, please see the aforementioned list of CFTC's PIAs.

2) Is a SORN required? If so, explain how the use of the information in this system is limited to the use specified in the SORN?

Depending on the content and how it is retrieved, information maintained in M365 may be covered by a number of CFTC SORNs. All CFTC SORNs are accessible at the aforementioned link.

VIII. INDIVIDUAL PARTICIPATION

1) Is the information collected directly from the individual?

Certain information in M365 may be collected directly from the public through

email.

2) Is the collection mandatory or voluntary? If voluntary, what opportunities do the individuals have to decline to provide information?

Collections that occur through email are voluntary. If an individual does not want to provide the information requested in the email they can decline to respond to the email.

3) Do individuals have an opportunity to consent to a particular use of the information? If so, how do they provide consent for a particular use?

The opportunity to consent depends on how the information is collected. The CFTC generally does not use M365 as a main tool to collect information, including PII, directly from the public. However, CFTC staff and contractors use M365 for business operations in furtherance of the CFTC's mission. To the extent information maintained in M365 applications incidentally includes PII, individuals will not have an opportunity to consent. To the extent that consent is required for the underlying collection, however, the CFTC will obtain any consent necessary. If the information is collected through email, the individual has an opportunity to consent to a particular use in the email response.

Information in M365 pertaining to CFTC staff is collected to authenticate end-users and manage administrative business functions including personnel security, human resources, emergency notifications, etc. All CFTC staff are required to have a M365 account. Staff do not have an opportunity to consent to the use of the log information for the user accounts.

IX. DATA MINIMIZATION

1) What steps were taken to minimize the collection of PII in the system?

To ensure the amount of PII collected is minimized, all CFTC staff must take security and privacy training before being granted access to CFTC systems and data. All staff must also agree to the IT Rules of Behavior. The setting for recording meetings using Teams has not been disabled.

X. DATA QUALITY AND INTEGRITY

1) How is data quality ensured throughout the information lifecycle and business processes associated with the use of the information?

☐ Cross referencing data entries with other systems
☐ Third party data verification
☒ Data taken directly from individuals
☐ Character limits on text submissions
☐ Numerical restrictions in text boxes
☒ Other: Due to the nature of the system and the anticipated broad use of email and Teams across the agency, it is the responsibility of each user to ensure the quality and integrity of the data.

XI. RETENTION

1) What are the retention periods for the information?

Information in M365 is maintained and/or destroyed in accordance with applicable CFTC records disposition schedules and General Records Schedules (GRS) that are approved by the National Archives and Records Administration (NARA). CFTC staff are informed of their recordkeeping responsibilities through training and meetings. Any information that is scheduled for disposal is destroyed in accordance with applicable records schedules, OMB, NARA, and NIST requirements.

XII. SECURITY

1) What types of administrative safeguards protect the information?
☒ Contingency Plan
☒ User manuals for the system
☒ Rules of Behavior
☒ Non-Disclosure or other contractual agreement
☐ Other:

2) What types of physical safeguards protect the information?
   ☒ Guards
   ☒ Identification Badges
   ☒ Biometric
   ☒ Cameras
   ☒ Physically secured space with need to know access
   ☒ Other: As a Microsoft hosted cloud solution, Microsoft provides the physical safeguards to their data centers.

3) What types of technical safeguards protect the information?
   ☒ User Identification
   ☒ Firewall
   ☒ Virtual Private Network (VPN)
   ☒ Multi-factor Authentication (MFA)
   ☒ Passwords
   ☒ Encryption - Cisco ESA for On-Prem Exchange mailboxes. Microsoft Email Encryption for Exchange Online mailboxes
   ☐ De-Identification
   ☐ Anonymization
   ☐ Other:

4) What monitoring, recording, and auditing safeguards are in place to prevent or detect unauthorized access or inappropriate use of the information?

   CFTC systems are continuously monitored to detect unauthorized access as part of CFTC's security program. Access is limited to those with a need to know who understand their responsibilities in handling this information to prevent inappropriate use of the information. More information regarding the types of logs generated by CFTC is available in the CFTC's Splunk PIA, available here.

5) Is this system hosted by a Cloud Service Provider (CSP)? Yes
   a. If yes, which one? Microsoft Azure
   b. If yes, has the system obtained a FedRAMP Authorization? Yes.

XIII. TRAINING

1) What privacy training is provided to users of the system?

   All CFTC personnel are subject to CFTC agency-wide procedures for safeguarding personally identifiable information and receive annual privacy and security training.