Privacy Impact Assessment
for
Microsoft Exchange 2016

April 20, 2021

System/Business Owner

Robert Resch

Reviewing Official
Charles Cutshall
Chief Privacy Officer
Commodity Futures Trading Commission

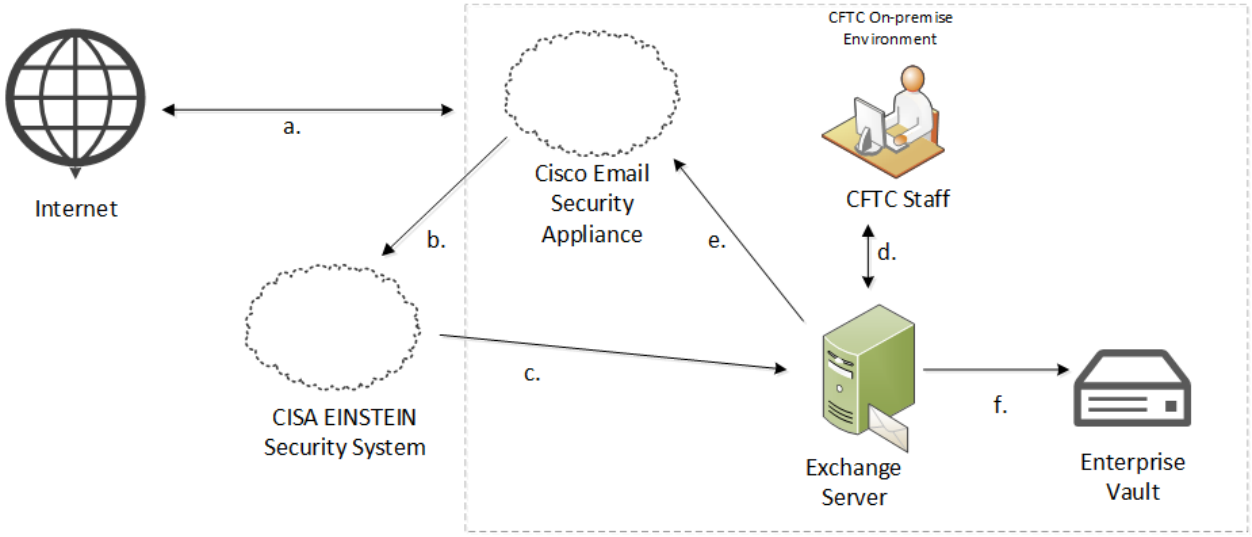
I. SYSTEM OVERVIEW

1) Describe the purpose of the system/collection:

Microsoft Exchange 2016 ("Exchange") is a remotely hosted enterprise messaging solution for email, calendar, and contacts used across the Commodity Futures Trading Commission ("Commission" or "CFTC"). Information collected, maintained, used, or disseminated by the Exchange includes end-user contact information, email messages (including any attachments), calendars, tasks, and audit log information. Even though end-users of the system are limited to CFTC employees and contractors, Exchange also captures information about non-CFTC individuals if non-CFTC individuals communicate or collaborate with a CFTC user. For example, if a non-CFTC individual communicates with a CFTC user via email, the email address of the non-CFTC individual, as well as any information transmitted through the email message, will be captured. In addition, in the performance of their duties, CFTC users may transmit information about non-CFTC individuals via this system, such as in the course of oversight and enforcement duties.

The Commission is in the process of transitioning to the Microsoft Office 365 Multi-Tenant & Supporting Services suite of products, which will include a separate cloud-based instance of Exchange. The Commission will continue to maintain Exchange 2016 in parallel until the transition is completed, at which time the system will be decommissioned and this PIA will be withdrawn.

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) US-CERT EINSTEIN security system. Read more about the EINSTEIN security system here: https://www.cisa.gov/einstein

c) Email which is cleared by EINSTEIN reaches the Exchange 2016 server within the CFTC's network boundary
d) CFTC staff receive and send email using their Outlook mailbox(es) that are connected to their Exchange account(s)
e) Outgoing mail is scanned by ESA (but not EINSTEIN) for certain types of sensitive personally identifiable information (PII).
f) Information in Exchange is moved to a separate archiving system, Enterprise Vault, when (i) CFTC staff manually mark content for archiving, (ii) an Outlook mailbox reaches 70% of its allotted storage capacity, and (iii) during the offboarding process for some CFTC staff.

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. Regarding use of EINSTEIN, see OMB Memorandum M-19-26, *Update to the Trusted Internet Connections (TIC) Initiative*, September 12, 2019.

III. INFORMATION TYPES

1) What information pertaining to CFTC end-users and members of the public will be collected, maintained, used, and/or disseminated?

Note: Information in Exchange is necessarily contextual and will depend on the nature of the communication. Information in Exchange could potentially include any of the following data elements or information types that are not specifically identified below. For example: Files pertaining to Human Resources (HR) may be emailed to another agency in support of CFTC's business operations, or information may be emailed to parties involved in enforcement actions. These are examples of how Exchange could be used, not necessarily how it is used.

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

IV. COLLECTING INFORMATION

1) How is the information in this system collected?

   Information is collected and stored on the Exchange server when an account is created and when the account is used to send and receive email. The information collected includes the content of email messages and any attachments, 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 Exchange as email attachments.

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 use Outlook mailboxes to retrieve information by CFTC end-user name and can retrieve other information (such as information contained in email messages) 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?

   Exchange does not itself require a SORN; however, SORNs that cover documents and records in Exchange that are considered part of Privacy Act systems are accessible 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?

   All CFTC staff members have Exchange accounts. In addition, multiple CFTC staff may be added to a shared mailbox to facilitate internal or external communication; staff with access to a group mailbox can both send and receive email from the group mailbox. CFTC staff may also create distribution lists to facilitate sending of notifications.

   Access to Exchange accounts is managed by the Division of Administration (DA), and each change in permissions or creation of a new account must be approved by DA and the relevant business unit.

   Access to Exchange log data is described in the CFTC's Splunk PIA, available here.

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

   The Exchange server has approximately 2,000 active accounts. Of these, approximately 1,100 are individual accounts for CFTC staff, and 900 are group accounts or distribution lists.

3) How is the information shared internally?

Information in Exchange can be shared internally using email or other collaboration tools such as SharePoint. Sharing of Exchange log data is described in the CFTC's Splunk PIA, available here.

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

CFTC staff communicating with non-CFTC parties in the proper course of their duties may share information by email. Information from Exchange may be shared externally in response to a FOIA request.

5) How is the information shared externally?

If CFTC staff must share sensitive CFTC information externally by email, they may mark such information as confidential using Exchange's confidentiality tools. If a confidential marking is applied, the non-CFTC party will be provided a link to securely view the information. The link is to open a connection to view the content and that connection is encrypted. The information is not included in or attached to the email itself and will remain at all times within the CFTC's network boundary.

Responsive documents to Freedom of Information Act (FOIA) requests may be shared by email, in hard copy, or by other media as necessary or convenient.

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 that they transmit through the computer or mobile device may be monitored, intercepted, searched, and/or seized by the Commission, and that users therefore have no reasonable expectation of privacy in such communications or other information. CFTF staff are referred to the Limited Personal Use Policy, which provides the same notice, when obtaining mobile devices issued by the Commission

To the extent that Exchange 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 assessment, (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.

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?

Exchange does not itself require a SORN; however, SORNs that cover documents and records in Exchange that are considered part of Privacy Act systems are accessible at: https://www.cftc.gov/Privacy/SORN/index.htm.

VIII. INDIVIDUAL PARTICIPATION

1) Is the information collected directly from the individual?

Yes, information is collected directly from CFTC staff in order to create their Exchange account.

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

All CFTC personnel are required to maintain an email account.

In some cases, individuals subject to the Commission's regulatory oversight may also be required to communicate with CFTC personnel using Exchange.

Other individuals are not generally required to communicate with the CFTC using Exchange; however, by not doing so, such individuals may be unable to receive communications the Commission chooses to only make available by email, participate in events hosted by the Commission, or benefit from other services provided by the Commission.

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?

Individuals are not able to consent to a particular use of information maintained in Exchange. They may, however, have an opportunity to consent to particular uses of information that is subsequently transferred to other information systems operated by the Commission.

IX. DATA MINIMIZATION

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

CFTC staff are obligated to abide by internal CFTC Rules of Behavior that restrict the type of information that can be shared by email.

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:

XI. RETENTION

1) What are the retention periods for the information?

   Exchange email and calendars for staff defined as Capstone Officials are maintained as permanent records of the Commission. At the time of departure, the Exchange inbox, sent mail, and calendars are saved to Relativity, which is an eDiscovery tool. CFTC holds the email for 15 years after the Capstone Official's departure. At the end of the 15-year period the email is transferred to the custody of the National Archives. See GRS 6.1, 010 (DAA-GRS-2014-0001-0001). Calendars are transferred from CFTC to the National Archives 30 years after the Official's departure. See DAA-0180-2018-0006-0001.

   Information in Exchange and Enterprise Vault for non-Capstone Officials is retained for 10 years and then destroyed. See GRS 6.1, 011 (DAA-GRS-2014-0001- 0002).

   System logs are maintained in accordance with GRS 3.2, item 030 and are destroyed when business use ceases.

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: None

3) What types of technical safeguards protect the information?
   - ☒ User Identification
   - ☒ Firewall
   - ☒ Virtual Private Network (VPN)
   - ☐ Multi-factor Authentication (MFA)
   - ☒ Passwords
   - ☒ Encryption
   - ☐ 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?

   Audit logs are maintained to help ensure compliance with tiered/role-based access as well as to help safeguard against unauthorized access, use, and disclosure of information. More information is available in the CFTC's Splunk PIA, available here.

5) Is this system hosted by a Cloud Service Provider (CSP)? No
   a. If yes, which one?
   b. If yes, has the system obtained a FedRAMP Authorization?

XIII. TRAINING

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

   Annual privacy and cybersecurity training, including periodic phishing security tests, is mandatory for all CFTC staff.