Privacy Impact Assessment
for the
Vulnerability Disclosure Program

April 20, 2021

System/Business Owner

Jack Wu

Reviewing Official
Charles Cutshall
Chief Privacy Officer

I. SYSTEM OVERVIEW

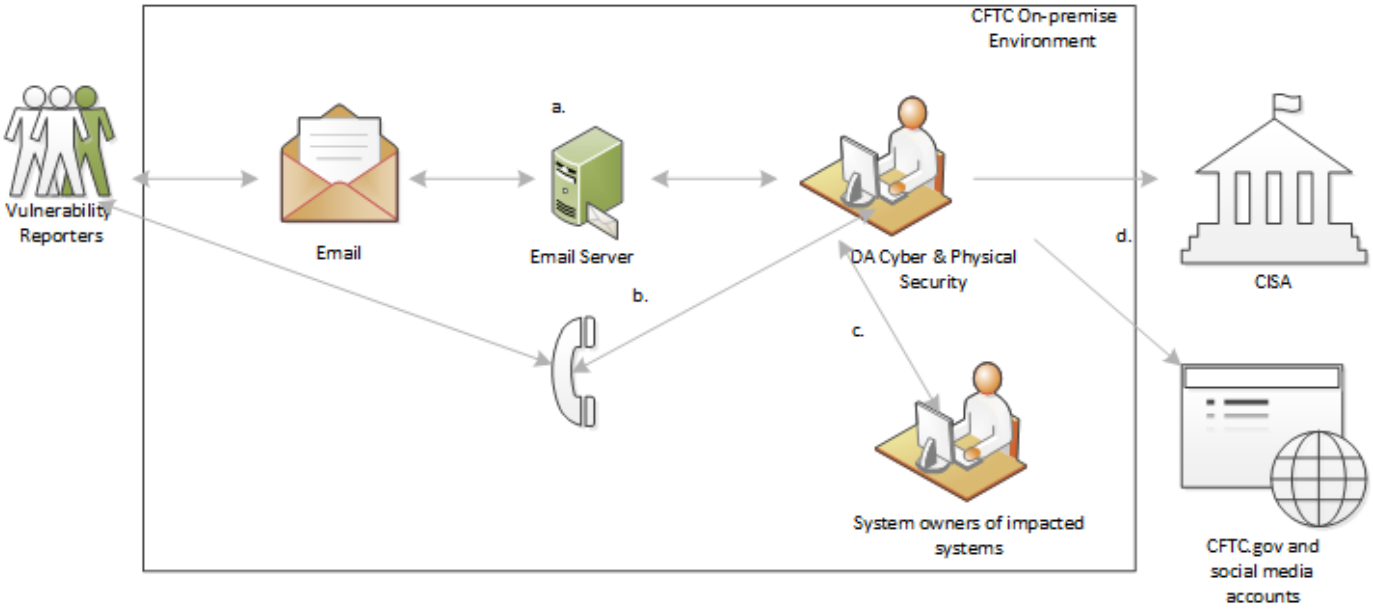
1) Describe the purpose of the system/collection:

The Commodity Futures Trading Commission ("CFTC" or "Commission") has created a Vulnerability Disclosure Program (VDP) to implement its Vulnerability Disclosure Policy that outlines specific practices for members of the public to follow when testing the security of certain CFTC information systems. The Vulnerability Disclosure policy is published on CFTC.gov and covers:

- what types of testing are authorized and for which information systems;
- where vulnerability reporters should send their reports;
- what type of information to include; and
- what to expect from the CFTC in response to a reported vulnerability.

Importantly, the CFTC will not recommend or pursue legal action related to any security research conducted in compliance with the VDP.

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. Vulnerability reporters submit their security research findings by email to Security_Vdp@cftc.gov.

b. CFTC staff from the Division of Administration's (DA) Cyber & Physical Security Branch review the vulnerability report and, if the vulnerability reporter consents, may request to communicate further about the vulnerability.

c. The vulnerability report may be forwarded to CFTC staff responsible for the security of relevant information systems.

d. If the vulnerability reporter consents, their contact information and findings may be shared with the Cybersecurity & Infrastructure Security Agency (CISA), an operational component

under Department of Homeland Security (DHS) oversight. At the vulnerability reporter's request, their name and contact information may also published on CFTC.gov or on CFTC social media accounts.

II. AUTHORITY AND PURPOSE

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

Department of Homeland Security Binding Operational Directive 20-01, *Develop and Publish a Vulnerability Disclosure Policy* (Sept. 2, 2020).

III. INFORMATION TYPES

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

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	
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 CFTC users of the system 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?

Vulnerability reporters submit reports to Security_Vdp@cftc.gov. Reports may include attachments. Further communications regarding the vulnerability are conducted by email, or if the vulnerability reporter consents, by telephone.

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.

V. INFORMATION USE

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

Emails from vulnerability reporters and their attachments are stored in Microsoft Exchange. Information related to reported vulnerabilities can be searched for and retrieved in Microsoft Exchange using the vulnerability reporter's name or email address.

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?

While information in the system is retrieved using one or more of the identifiers documented above, the information retrieved is not about the vulnerability reporter and therefore does not trigger the notice requirements of the Privacy Act.

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?

   Access to the Security_Vdp@cftc.gov inbox is limited to members of the DA Cyber & Physical Security Branch with a need to know.

2) How is the information shared internally?

   Emails from vulnerability reporters may be forwarded to CFTC staff responsible for the security of relevant information systems.

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

   With the vulnerability reporter's consent (e.g., in the course of email exchanges with CFTC staff), their name and contact information may be shared with CISA.

4) How is the information shared externally?

   The vulnerability reports and subsequent communications with the vulnerability reporter are forwarded by email to CISA. At the vulnerability reporter's request, their name and contact information may also published on CFTC.gov or on CFTC social media accounts.

VII. TRANSPARENCY

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

   Information about the Commission's VDP, including what information will be collected and with who it will be shared, is publicly available through CFTC.gov. In addition, this assessment serves as further notice of how information related to vulnerability reporters will be collected, used, and shared.

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?

   A SORN is not required.

VIII. INDIVIDUAL PARTICIPATION

1) Is the information collected directly from the individual?

   Yes, information is collected directly from the vulnerability reporter.

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

   The collection is voluntary. There is no obligation for vulnerability reporters to test for vulnerabilities on CFTC information systems.

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?

   Vulnerability reporters may consent to have their name and contact information be shared with CISA.

IX. DATA MINIMIZATION

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

   The policy prohibits vulnerability reporters from including any personal information accessed during their testing in the vulnerability report. The policy also requests that vulnerability reporters not provide any personal information beyond their name and contact information when submitting vulnerability reports, and allows them to submit vulnerability reports anonymously, in the colloquial sense.

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?

Records of vulnerability reporting are covered by General Records Schedule 3.2, item 020, Systems and Data Security Records. This schedule includes records related to information system risk management and vulnerability analyses. Records are destroyed 1 year(s) after system is superseded by a new iteration or when no longer needed to ensure a continuity of security controls throughout the life of the information system.

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 is mandatory for all CFTC staff. In addition, DA Cyber & Physical Security Branch staff with access to the Security_Vdp@cftc.gov inbox are instructed to only share information in accordance with the VDP.