Commodity Futures Trading Commission
Privacy Impact Assessment

System Name: Enterprise Asset Management System

Office: Business Management and Planning, Logistics and Operations

Date: May 10, 2019

1. Overview

The Business Management and Planning/Logistics and Operations Section in coordination with the Office of Data and Technology is implementing a new hosted asset/property management system. The system will strengthen regulation reporting and agency compliance, and enhance effectiveness of internal controls to prevent fraud, abuse, or mismanagement of CFTC assets.

The asset management system will cover the CFTC headquarters and all field locations and enable managing the full life-cycle of events and transactions performed against CFTC accountable assets. Accountable assets are primarily Information Technology equipment such as desktops and laptop PCs, desk phones, mobile devices including smartphones and tablets, audio visual equipment, printers, data servers, switching devices, and non-IT assets such as artwork, ice makers, and other tangible items (e.g., HVAC units).

The system will provide a secure process for handling assets, provide the ability to automate workflows, reconcile assets through hand held scanners, and generate a number of required compliance reports and forms to effectively manage the assets throughout the asset management lifecycle.
The personal information collected in the system is limited to individual names that are linked to specific assets, the office location of the asset (which may be linked to the location of the individual, such as their office room), and basic log-in information for users of the system including username and password.

2. Data Collected and Stored Within the System

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

The following data will be collected, used, disseminated, and maintained in the system:

1. PII Categories	2. Is collected, processed, disseminated, stored and/ 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				
Social Security Number (SSN, last 4 digits)				
Tax Identification Number (TIN)				
Photographic Identifiers				
Driver's License				
Mother's Maiden Name				
Vehicle Identifiers				
Mailing Address				
E-Mail Address	X	X		X
Phone Number	X	X		X
Medical Records Number				
Medical Notes or some other Health Information				
Financial Account Information				
Certificates				
Legal Documents				
Device Identifiers	X	X		X
Web Uniform Resource Locator(s)				
Education Records				
Military Status				
Employment Status				
Foreign Activities				
Description and Physical office Location of Asset	X	X		X
Username and password for users	X	X		X
Office Location of Asset Assignee	X	X		X
Title/Position/Role of User	X	X		X

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

The personal information is extracted from existing CFTC sources, such as Active Directory, or input by CFTC staff.

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

The information is collected to track the acquisition, control, use, and disposition of Government property. The system provides information on the location and the individual responsible for the Government property assigned to them.

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

Assets are entered into the system by CFTC employees and contractors. As part of the onboarding process, assets are assigned to individuals by specific employees or contractors with that responsibility. The information is updated when the employee moves, departs, or changes are made to the assets assigned.

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 the CFTC has not previously employed. The system does not monitor individuals.

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

CFTC has the authority to collect the information as it relates to the acquisition, control, use, and disposition of Government property under these authorities:

- GSA Federal Management Regulations, Chapter 102, Sub-Chapter B
- Federal Property and Administrative Services Act of 1949 (as amended), §202, 40 USC §483(b)
- Office of Management and Budget (OMB)/Joint Financial Management Improvement Program Property Management System Requirements
- OMB/Federal Accounting Standards Advisory Board Statement of Federal Financial Accounting Standards 3, 6, 8, 11 and 16
- OMB Memorandums, Bulletins, and Circulars 01-09, A-11, A-123, A-127, and A-130

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?

The information will be stored in electronic form throughout the lifecycle of the asset and retained for 2 years after the asset is disposed of and/or removed from the agency's financial statement per GRS 1.1, item 030

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

The information will be securely deleted in accordance with the disposition periods stated above in the answer to question 3.1.

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)?

Federal employees and contractors with a role in managing, assigning, or depreciating assets will have access to the information based on their role. Data is shared with other employees or contractors who have a role in asset management or internal controls on a need to know basis. Contractors are subject to confidentiality requirements and those subject to the Federal Acquisition Regulations ("FAR") are subject to FAR clauses concerning the Privacy Act, 52.224-1 and 52.224-1.

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

The data will not be shared outside the Commission to anyone other than contractors who help manage the system. All sensitive information transferred to the contractors will be encrypted.

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 information to fulfill their job responsibilities, e.g., contractors responsible for managing the solution, this data 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 is not aware of any other data set that could be used to re-identify the information in this system.

.

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.

The CFTC does not intend to share personal information from this system to outside entities. If required, the CFTC will be able to track the disclosure from the original request including date, nature, and purpose of disclosure through system search queries to identify the disclosed data and activity logs to understand the date, nature, and purpose of disclosure.

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. Other CFTC systems do not share the information or have access to the information in this system.

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?

Notice is provided by this PIA and the SORN CFTC- 46, Lost, Stolen, Damaged or Destroyed CFTC Property.

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?

To receive a CFTC asset, the asset recipient must provide information to link the asset to the individual recipient. If the recipient declines to provide the information, the CFTC cannot issue them an asset.

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?

If an individual would like to gain access to records contained in a Privacy Act system of records, they can obtain access or request amendment by following the procedures 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?

The 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. The asset management system is only accessible from within the CFTC network which requires PIV card login. In addition, the asset management system requires the use of a unique username and password.

Physical security measures include restrictions on building access to authorized individuals 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?

CFTC performs a complete inventory every three years with a minimum of 10% annually to validate the information in the system. The operational nature of the system requires the data to be constantly evaluated to enable accurate tracking of assets.

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

No. The system has the capability to identify the CFTC asset issued to a specific individual. The system includes a location for the asset, which in certain cases may be the office location of an individual, but the solution does not have the ability to locate or monitor individuals in real-time.

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

Yes. The system complies with FISMA requirements. The system is FedRAMP authorized to help ensure the information is appropriately secured.

6.5. Describe the privacy training provided to users either generally or specifically relevant to the program or system.

All CFTC employees and contractors are subject to CFTC agency-wide 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, information may be retrieved by name to verify assets assigned to them, usually upon departure, relocations, or other changes regarding the assets themselves.

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 information is covered under SORN CFTC–46, Lost, Stolen, Damaged, Destroyed Property/

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 data in this system pertains to CFTC employees and contractors only and not members of the public. The CFTC Privacy Policy on CFTC.gov is not directly applicable in this case. The collection, use, and disclosure of information are consistent with the Privacy Act, OMB requirements, CFTC regulations, and internal policies and procedures for handling personal 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?

Given the type of personal information in the system (name, office location) the system presents a low privacy risk with measures in place to limit access and secure information.

There is a risk of collecting too much information for the specific purpose of this system. To mitigate this risk, the CFTC Business Management and Planning Office reviewed the information required for the system with the Privacy Office to determine the minimum amount necessary to be included in the system to accomplish its purpose.

There is a risk that those with authorized access could use their access for unapproved or inappropriate purposes. To mitigate this risk, the solution contains a complete history of the activities performed by all users. Any inappropriate use that is identified from this history is investigated and if necessary, referred to the appropriate internal investigators (such as the CFTC Office of Inspector General or others as required) for handling.

.