# Commodity Futures Trading Commission
# Privacy Impact Assessment

**System Name:** Management and Administrative Enterprise Database (MAED)

**Office:** Office of Data and Technology (ODT)

**Date:** May 10, 2019

## 1. Overview

The Management and Administrative Enterprise Database (MAED) is an internal CFTC system that helps facilitate administrative business processes within the Commission and provides a platform to centrally store and manage CFTC staff member (employee and contractor) and vendor data. MAED contains staff member, vendor, contract, and budget information used in day-to-day operations by multiple CFTC systems. The system consolidates the workforce and business-related system databases into a centralized data repository and unifies data retrieval through enterprise data services. The result is improved maintainability, interoperability, data security, data quality, data integrity, and ad-hoc query capability.

The foundation of the MAED platform is the MAED Database which provides data securely to a number of subsystems. A key attribute of the MAED system is its service architecture which provides a collection of services that enable data to be made available to MAED subsystems for use in CFTC applications. MAED's standard subsystems consist of a central website and supporting components which use the MAED services platform for data needs.
These subsystems include:

| System | Acronym | Description |
|---|---|---|
| Emergency Contact System | EContact | The Emergency Contact System allows certain CFTC staff to contact an employee or contractor as well as an individual the employee or contract designates as an emergency contact in case of an emergency. This information is input directly into the system by the employee or contractor. The system also allows CFTC to send automatic notifications to employees and contractors of building closures and other significant events. |
| Learning Management System Tools | LMS | This set of processes and solutions includes a process that updates the CFTC's Learning Management System (LMS) with CFTC employee profiles on a daily basis through Application Programing Interface (API) services; a process that consolidates information from the LMS and MAED to submit to OPM; and a solution that enables Single Sign On to the LMS. |

| System | Acronym | Description |
|---|---|---|
| Offboarding System | | The Offboarding System notifies CFTC offices that a CFTC contractor is departing and tracks post-offboarding activities. |
| Personnel Clearance System | PCS | The Personnel Clearance System (PCS) manages information about security clearances. The application tracks security investigations as they advance through the approval process. It also sends email alerts about security investigation actions and processing deadlines. Although PCS does not automatically submit background investigation forms to the Office of Personnel Management (OPM), it allows tracking of documents submitted to OPM and to track security investigations. |
| Relationship Hierarchy Manager | RHM | The Relationship Hierarchy Management (RHM) system supports staff hierarchies by allowing CFTC staff to track and edit COR/contract/contractor, supervisor/employee, contracting officer/contracts relationships. |
| Vendor and Contract Management System | VCMS | The Vendor and Contract Management System (VCMS) maintains data about vendors and contracts and assists with matching awarded contracts with CORs and facilitates the management and tracking of vendor information. |
| Workforce Change Request | WCR | Workforce Change Request (WCR) allows business managers, directors, and supervisors to request changes to employee information, status, location, and resources. The information is used to move the employee and/or make any changes to equipment or network access that may be required due to the change. |

## 2. Data Collected and Stored Within the System

2.1. What information will be collected, used, disseminated or maintained in the system?
MAED and its subsystems contain administrative management, financial management, and supply chain management information.

| 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 | x |
| Date of Birth | x | x | | x |
| Social Security Number (SSN, last 4 digits) | x | x | | x |

| | | | | |
|---|---|---|---|---|
| Tax Identification Number (TIN) | | | | |
| Photographic Identifiers | | | | |
| Driver’s License | | | | |
| Mother’s Maiden Name | | | | |
| Vehicle Identifiers | | | | |
| Mailing Address | x | x | | x |
| E-Mail Address | x | x | x | x |
| Phone Number | x | x | x | x |
| Medical Records Number | | | | |
| Medical Notes or some other Health Information | | | | |
| Financial Account Information | | | | |
| Certificates | | | | |
| Legal Documents | | | | |
| Device Identifiers | | | | |
| Web Uniform Resource Locator(s) | | | | |
| Education Records (Training) | x | x | | x |
| Military Status | x | x | | x |
| Employment Status | x | x | | x |
| Foreign Activities | | | | |
| Other: employment action data from SF 52 forms | x | x | | |

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

The information in MAED is collected from CFTC staff, the National Finance Center and from Recruit 2 Hire (R2H), a human resources information system that captures SF-52 information for Federal employees.

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

This information is necessary to conduct the administrative functions of the CFTC pertaining to the CFTC staff members, including such functions as conducting security background checks, distributing benefits, and tracking employment of CFTC staff members.

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

The information is collected through web interfaces of internal systems, when the source is the CFTC staff, and from SQL Server Integration Services (SSIS) packages bringing information from other systems, such as the National Finance Center database.

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

No. The technology used by MAED systems is established and commonly in use in the CFTC. MAED does not have the ability to monitor individuals.

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

For collection of employee personnel, payroll, time, and attendance records: 5 U.S.C. §§ 6101-6133; 5 U.S.C. §§ 6301-6326; 44 U.S.C. § 3101.

For collection of emergency contact information: 5 U.S.C. § 301.

For background investigation information: 5 C.F.R., parts 731, 732, and 736; Exec. Order No. 10450, “Security Requirements for Government Employment," 18 Fed. Reg. 2489 (Apr. 27, 1953). The Office of Personnel Management (OPM) is authorized to collect this information under 5 U.S.C. §§ 3301, 3302, and 9101. 5 U.S.C. § 1104 allows OPM to delegate the personnel management function to other Federal agencies.

For collection of contractor information: 5 U.S.C. § 301; the Office of Federal Procurement Policy Act (41 U.S.C. § 405).

For collection of training records: 5 U.S.C. § 4103; 5 C.F.R., parts 410 and 412; E-Government Act of 2002, Pub. L. No. 107-347; Exec. Order No. 11348, “Providing for the Further Training of Government Employees,” 32 Fed. Reg. 6335 (Apr. 20, 1967); Exec. Order No. 13111, “Using Technology to Improve Training Technologies for Federal Government Employees,” 64 Fed. Reg. 2793 (Jan. 15, 1999).

For general personnel records: 5 U.S.C. §§ 1302, 2951, 3301, 3372, 4118, and 8347; Exec. Order No. 9397, as amended by Exec Order No. 13478, “Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers,” 73 Fed. Reg. 225 (Nov. 20, 2008) and Exec. Order No. 9830, “Amending the Civil Service Rules and Providing for Federal Personnel Administration,” 12 Fed. Reg. 1259 (Feb. 24, 1947); Exec. Order No. 12107, “Relating to the Civil Service Commission and Labor-Management in the Federal Service,” 44 Fed. Reg. 1055 (Dec. 28, 1978).

For employee performance file system records: 5 U.S.C. §§ 1104, 3321, 4305, and 5405; Exec. Order No. 12107.

For collection of records of adverse actions, performance based reductions, in grade and removal actions, and terminations of probationers: 5 U.S.C. §§ 3321, 4303, 7504, 7514, and 7543.

## 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?

All records are maintained electronically and retained for the period of time indicated in the below retention schedules.

| Records | Retention |
|---|---|
| Emergency Contact | Emergency contact information is categorized under General Retention Schedule (GRS) 5.3, item 020 Employee emergency contact information. This information is required to be destroyed when superseded or obsolete, or upon separation or transfer of employee. |
| Learning Management System | A six (6) year retention is imposed for all training records consistent with GRS 2.6, item 010. Business use requires a longer retention period of 6 yrs. GRS 2.6, item 010 states "Destroy when 3 years old, or 3 years after superseded or obsolete, whichever is appropriate, but longer retention is authorized if required for business use." |
| Off-boarding | The Off-boarding system tracks the off-boarding process. This information is considered intermediary records and follows GRS 5.2, item 020 – Intermediary records. The records are destroyed upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.<br>Contractor records documenting post-off-boarding activities are considered part of the contract records and are not stored in the Off-boarding system that contains only tracking information about the process. |
| Personnel Clearance | Personnel clearance records are categorized under GRS 5.6, Item 181 and are required to be destroyed five years after the individual's relationship with the CFTC ends. |
| Relationship Hierarchy | Relationship Hierarchy records are considered intermediary records and categorized under GRS 5.2, item 020 – Intermediary Records. Records are required to be destroyed upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later. |
| Vendor and Contract Management | The tracking information related to vendor and contract management records follow the same retention schedule as the substantive contract documents, which pursuant to GRS1.1, item 010 are to be destroyed 6 years after final payment or cancellation, but longer retention is authorized if required for business use. |
| Workforce Change Request | The workforce change request records are considered Administrative Records, retained by any agency office and are to be destroyed according to GRS 5.1, item 010: Administrative Records, and destroyed when business use ceases. |

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

Data in the MAED system will be retained according to the approved retention schedules outlined above. All data is destroyed using secure destruction methods.

## 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)?

Data is accessed primarily by Federal employees who have a need to know, as determined by their business role. Contractors have access to the database as necessary for operations and maintenance. CFTC contractors with access to the MAED 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.

Data is shared from MAED with the Office of Personnel Management in order to report training data, and the emergency notification system uses the personal contact information from MAED. In addition, 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 MAED system in accordance with the applicable Privacy Act System of Records Notices. The CFTC provides notice to employees of these possible disclosures, as discussed below in Section 5.1.

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

Data from the MAED system is shared electronically using secure transfer methods. Training data sent to the Office of Personnel Management is transferred using ConnectDirect FTP+, a secure FTP protocol, and TLS 1.2.
Contact information sent to Send Word Now is sent via the HTTPS web service endpoint.

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 data sent to OPM, and the hosted training vendor, this data is never sent to the public, consultants, researchers, or other such third parties.

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 information in the system is not sent to recipients in aggregated or de-identified form.

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 is able to track disclosures of personal information from the MAED system through system logs and data export documentation that indicates what information was exported or shared from the system.

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)?

Data from MAED is shared or made available to CFTC systems outlined below.

| **System Name** | **Data Direction (incoming, outgoing, both)** | **Information being transmitted** |
|---|---|---|
| Cornerstone On Demand Learning Management System (LMS) | Both | Outgoing: Staff member name (Both Employee and Contractor), supervisor, employment status, grade, organization, bargaining unit status, and region<br>Incoming: Employee ID, training specific records (e.g., title, type, duty hours, start/end date, delivery type) |
| EContact | Outgoing | Staff Member and Staff Member's Emergency Contact Information (personal phone number, email, mobile number, and name) |
| Training Event Registration (TERS) | Outgoing | Training specific records (e.g., title, type, duty hours, start/end date) |
| National Finance Center (NFC) | Incoming | Payroll, SSN, Organization Information |
| Recruit to Hire (R2H) | Both | SF52 internal ID, NOA, Position Data |
| Active Directory | Both | AD group membership, email, room number, location, organization |

| System Name | Data Direction (incoming, outgoing, both) | Information being transmitted |
|---|---|---|
| eLaw Practice Manager | Incoming | Budget Planning and Activity Code (BPAC)[1], Matter Name |
| Legal Files | Incoming | BPAC, Matter Name |
| Application Management Tool (AMT) | Incoming | Supervisor Name |
| StatusReport | Outgoing | Supervisor Name |
| Master Data Services (MDS) | Outgoing | Staff Member Name, Email |
| Training Log | Outgoing | To OPM by manual process: SSN (from NFC), training specific records (e.g., title, type, duty hours, start/end date, delivery type, cost,) |
| Business Information System (BIS) Process | Outgoing | Staff Member Name, Employee ID |

## 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?

Specific notice is provided by Privacy Act statements and notices that are displayed on the collection instruments when the data is collected directly from the individual including on the LMS, the EContact system, and various employee forms that become part of the employee's personnel file. In addition this PIA and the corresponding SORNs included in 7.2 below provide additional notice.

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?

If a Privacy Act statement is required, it will indicate whether the collection is voluntary or mandatory. An individual can decline to provide information, but it may impact the benefits and services offered to the individual.

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?

[1] BPAC data enables the CFTC to gather detailed information on all CFTC activities to be used by agency program managers in their resource management activities and budget formulation.

An individual can follow the process outlined at CFTC.gov/privacy and 17 CFR 146.8 to file a Privacy Act request to request amendment/correction to Privacy Act records.

## 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?

Unauthorized access is prevented by the use of Active Directory groups to control user roles. Each role is limited to only the information necessary to carry out the business function of that role. In addition, for most of the data, access is provided through services which limit direct access and modifications to the underlying database. Users with regular access to sensitive PII are required to take specific training on how to handle PII. All users must also abide by IT Rules of Behavior and take annual required Security and Privacy Training.

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?

MAED data is constantly updated and used regularly. If any information is missing or incorrect, it is noticed and corrected during normal business interactions. The information received from the National Finance Center is updated every two weeks.

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

The system does not provide the capability to locate an individual in real-time or monitor an individual. The system provides the capability to identify an individual and includes contact information that may include business and personal address.

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

Yes. The CFTC follows applicable FISMA requirements to ensure that the information found in MAED is appropriately secured.

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

All CFTC personnel are subject to CFTC agency-wide procedures for safeguarding PII and receive annual privacy and security training. The Human Resources Branch, who are frequent users of the system, also receive additional role-based training regarding protecting PII.

## 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. The data in the system is retrieved by personal identifier such as a name, unique employee ID, or SSN.

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 data in the system is covered by a number of CFTC and Government-wide SORNs:

CFTC-5, Employee Personnel, Payroll, Time, and Attendance
CFTC-9, Emergency Locator System
CFTC-35, General Information Technology Records
CFTC-44, Personnel Clearance System
CFTC -51, Contractors and Consultants
CFTC -52, Training Records
OPM SORN GOVT-1 General Personnel Records
OPM SORN GOVT-2 Employee Performance File System Records
OPM SORN GOVT-3 Records of Adverse Actions, Performance Based Reductions In Grade and Removal Actions, and Terminations of Probationers

## 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 Privacy Office confirms that the collection, use, and disclosure of the information in this system have been reviewed to ensure consistency with the CFTC’s Privacy Policy and the information contained in this system is consistent with Federal government and CFTC requirements for collection, use, and disclosure of the 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?

There is a risk the staff that have access to the data may use it for a different purpose. To mitigate this risk, access to information is limited to those with a need to know to perform their specific business function. Access to the data is provided through services, which limits direct access and modification to the underlying database.

There is a risk that information will be retained for longer than is needed to accomplish the purpose for which the information was originally collected. To mitigate this risk, the CFTC has implemented retention schedules approved by NARA with regularly scheduled deletion cycles. See section 3 regarding data retention.

There is also a risk of unauthorized or inadvertent disclosure of this data. To mitigate this risk, access to information is limited to those with a need to know and controlled systematically by Active Directory. The data is encrypted at rest, and sensitive personally identifiable information is encrypted at the record level.

There is a risk that the data may be inaccurate. Most of the data in the system is provided directly by the individual, so there is an assumption that it is accurate.
To ensure the reliability of the data, the data is regularly updated using the MAED system during the course of business, and data from the National Finance is refreshed every two weeks.

There is a risk that authorized users, such as the Human Resources Branch are exposed to PII as a routine part of their official duties. These users may make inappropriate disclosure of this information, either intentionally or unintentionally. To mitigate this risk, users with regular access to sensitive PII are required to take specific training on how to handle PII. All users must also abide by IT Rules of Behavior and take annual required Security and Privacy Training.