Commodity Futures Trading Commission
Privacy Impact Assessment

System Name: Application Management Tool (AMT)

Office: Office of Data and Technology (ODT)

Date: May 10, 2019

1. Overview

The Commodity Futures Trading Commission (CFTC) developed the Application Management Tool (AMT) to provide a central interface to access employee data to assign roles and manage access within specific administrative and management systems. AMT provides an authorization framework to various CFTC subsystems based on the role and/or organization relationship. The tool helps facilitate ethics tracking, purchase tracking, training management, performance management, and pay adjustments for CFTC employees.

AMT subsystems are designed with the same general pattern and approach. Each sub-system contains a website and an associated database. Access controls for each subsystem are based on a need to know basis dependent upon a particular user's role and responsibilities within the CFTC.

AMT includes the following subsystems and system components:

- Annual Payment Adjustment Calculator (APAC)
- Ethics Management and Tracking (EMAT)
- Performance Management Program (PMP)
- Purchase Card Tracking System (PCTS)
- Training and Events Registration (TERS)

System	Acronym	Description
Annual Payment Adjustment Calculator	APAC	APAC is a tool that allows CFTC staff to work with employee and pay factor data to perform annual adjustments to CFTC employee pay. It also generates pay adjustment processing lists and employee pay adjustment letters. The tool includes SSN, salary, name, location, grade information.
Ethics Management and Tracking	EMAT	EMAT enables the online filing of financial disclosure forms 185, 450, and 450A.
Performance Management Program	PMP	The PMP provides CFTC staff the functionality to enter, modify, and report on employee performance assessment data.

System	Acronym	Description
Purchase Card Tracking System	PCTS	The PCTS creates work-related purchase requests, and provides a consistent means to collect, maintain, and display purchase card-related information.
Training and Events Registration	TERS	TERS allows users to invite selected users to training and event sessions, and allows employees and contractors to sign up for the events and training.

2. Data Collected and Stored Within the System

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

AMT and its subsystems include information about CFTC employees' financial disclosures, details about the financial transactions involving CFTC purchase cards, details of payroll information, performance evaluations of CFTC employees, and training registration information for employees and contractors.

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	X	X		
Tax Identification Number (TIN)				
Photographic Identifiers				
Driver's License				
Mother's Maiden Name				
Vehicle Identifiers				
Mailing Address	X	X		
E-Mail Address	X	X		X
Phone Number	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				
Employment Status	x	x		
Foreign Activities				
Financial disclosure Information	x	x		
Purchase Card Information	x	x		
Payroll and Salary Information	x	x		
Performance Evaluations	x	x		

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

The information in AMT is collected from:

- CFTC staff members
- National Finance Center (NFC)
- Management and Administrative Enterprise Database (MAED) System
- Active Directory

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

This information is necessary to conduct the administrative functions of the CFTC including recording purchase card transactions, salary adjustments, financial disclosures under Title I of the Ethics in Government Act, tracking performance evaluations, and conducting and reporting training.

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 through internal integrated services that pull information from other CFTC systems.

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 AMT is established and commonly in use in the CFTC. AMT does not have the ability to monitor individuals.

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

The CFTC is authorized to collect this information pursuant to the following authorities:

For 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"; Exec. Order No. 13111, "Using Technology to Improve Training Technologies for Federal Government Employees."

For financial disclosure Information: Title I of the Ethics in Government Act of 1978, Pub. L. No. 95-521; Exec. Order No. 12674, "Principles of Ethical Conduct for Government Officers and Employees", as modified by Exec. Order No. 12731, "Standards of Ethical Conduct for Employees of the Executive Branch; Amendment to the Standards Governing Solicitation and Acceptance of Gifts from Outside Sources"; 5 C.F.R., part 2634, subpart I (subject to prior written approval of the Director of the Office of Government Ethics, authorizes the collection of the information on the OGE Form 450). The legal basis for the Certification of Compliance with the Commission's Conduct Regulation, CFTC Form 185, is found in sections 2(a)(7) and (11), and 8a(5) of the Commodity Exchange Act, as amended (7 U.S.C. §§ 4a(f) and (j), and 12a(5)).

For payment card information: Exec. Order No. 9373; Exec. Order No. 12931, "Federal Procurement Reform; 40 U.S.C. §§ 501-502.

For performance management information: 5 U.S.C. §§ 1104, 3321, 4305, and 5405; Exec. Order No. 12107, "Relating to the Civil Service Commission and Labor-Management in the Federal Service."

For pay rate adjustment information: 5 U.S.C. §§ 6101-6133; 5 U.S.C. §§ 6301-6326; 44 U.S.C. § 3101.

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 per the NARA-approved General Retention Schedule (GRS).

Records	Retention
Records used to calculate pay rate adjustments	Records used to calculate payroll and pay rate adjustments are categorized under GRS 2.4, Item 01. These records are to be destroyed 2 years after employee separation or retirement, but longer retention is authorized if required for business use.
Financial Disclosure Form data	Financial disclosure records such as the records from the EMAT subsystem are covered under GRS 2.8, Items 070, 071, 072, 100 and 101 depending on the disclosure form from which the information is derived.

Records	Retention
Performance Management Records	Performance management records are covered under GRS 2.2 items 070 and 071. Item 070 pertains to acceptable performance appraisals of non-senior executive service employees and requires destruction 4 years after date of appraisal, but longer retention is authorized if required for business use. Item 071 applies to unacceptable performance appraisals of non-senior executive service which are required to be destroyed after employee completes 1 year of acceptable performance from the date of written advance notice of proposed removal or reduction-in-grade notice.
Payment Card Records	Payment Card records are covered under GRS 1.1, Item 010 and are scheduled to be destroyed 6 years after final payment or cancellation, but longer retention is authorized if required for business use.
Training Records	Training records are currently covered under GRS 2.6, Items 010, 020, 030 and are to be destroyed after 6 years, or when superseded, whichever is later.

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

Data in the AMT 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, as determined by their business role. Some contractors have access to the database as necessary for operations and maintenance. In addition, some contractors have access to the data required to carry out the administrative functions for which they are responsible. Data is also shared from AMT systems with the Office of Personnel Management in order to report training data.

The CFTC may also share the information in the AMT 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.

CFTC contractors with access to the AMT 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.

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

The only data that is shared outside the Commission is training related data required by OPM. Data from the AMT 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.

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, this data is never disclosed 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 information in this 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.

Disclosures other than to OPM are not anticipated, but a disclosure from the system can be tracked back from the original request through export logs and manually back tracking the disclosure through 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)?

As outlined below, the AMT system shares or makes available information pertaining to the following internal CFTC systems:

System Name	Data Direction (incoming, outgoing, both)	Information made available or transmitted
Active Directory (AD)	Both	AD group membership, email, room number, location, organization

System Name	Data Direction (incoming, outgoing, both)	Information made available or transmitted
National Finance Center (NFC)	Incoming	Payroll, SSN, Organization
ELaw Legal Files	Incoming	BPAC, Matter Name
MAED	Both	Employee ID, Name, Grade, Supervisor name

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?

Privacy Act statements or notices are displayed on the collection instruments when the data is collected directly from the individual. Statements are included on initial employee forms or on systems that required manual data input such as EMAT. Additionally, this PIA and the separate system PIAs such as for EMAT, ELaw, and MAED provide notice as well as the general notice included in the SORNs listed in question seven below.

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?

The Privacy Act statements 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?

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?

The information is protected from misuse and unauthorized access through various administrative, technical, and physical security measures. Roles within AMT are controlled by a sub-system of AMT, where system administrators can assign roles to

CFTC staff. Each role is limited to only the information necessary to carry out the business function of that role.

Users with regular access to sensitive PII, such as the Human Resources Branch, 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. Other general technical security measures within CFTC include restrictions on computer access to authorized individuals, required use of strong passwords frequently changed, use of encryption for certain data types and transfers, and regular review of security procedures and best practices to enhance security.

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?

AMT data is regularly updated and used on a consistent basis. If any information is missing or incorrect, it is noticed and corrected during normal business interactions.

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 in some instances determine his/her 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 AMT 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. Role-based training is provided for certain functions such on Human Resources Branch personnel who may have regular access to personal information to perform their job function.

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 will be retrieved by a personal identifier such as name, employee ID, or SSN in the normal course of business.

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. These include:

CFTC-5, Employee Personnel, Payroll, Time, and Attendance
CFTC -52, Training Records
OPM/GOVT-2 Employee Performance File
OPM/CENTRAL-13 Executive Personnel Records
OGE/GOVT-2, Executive Branch Confidential Financial Disclosure Reports
GSA/GOVT-6 GSA SmartPay Purchase Charge Card Program

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?

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. In addition, when data needs to be linked to individual, less sensitive unique identifiers such as employee ID are used instead of SSN.

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 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 Resource 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.