Commodity Futures Trading Commission
Privacy Impact Assessment

System Name: Learning Management System (LMS)

Office: Office of Executive Director (OED), Human Resources Branch (HRB)

Date: April 12, 2018

1. Overview

The Human Resources Branch in coordination with the Office of Data and Technology has procured a 3rd party hosted Learning Management System (LMS) from Cornerstone Inc. (Cornerstone). The LMS will assist the CFTC in the administration, documentation, tracking, reporting and delivery of educational courses or training programs. The intent is to help deliver material and administer training to CFTC Staff (employees, contractors, volunteers, and interns) to track progress and assist in record-keeping of training activities. The LMS will enable content delivery in a variety of forms, acting as a platform for fully online courses, as well as several hybrid forms, such as blended learning and in-person classroom sessions.

2. Data Collected and Stored Within the System

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

The system stores training information (courses, training rooms, instructors, and training completion history), personally identifiable information (PII), and human resource (HR) information for CFTC Staff.
Specific categories of PII may include:

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 (for purposes other than contacting federal employees)	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				
Personal Mailing Address				
Personal E-Mail Address				
Personal Phone Number				
Medical Records Number				
Medical Notes or some other Health Information				
Financial Account Information				
Certificates (Training)	**X**	**X**		**X**
Legal Documents				
Device Identifiers				
Web Uniform Resource Locator(s)				
Education Records	**X**	**X**		
Military Status				
Employment Type	**X**	**X**		**X**
Foreign Activities				
Other: Employee Bargaining Unit Status	**X**	**X**		
Other: Employee ID	**X**	**X**		**X**

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

The staff member names, employment type (contractor or Federal employee), and bargaining unit status will come from CFTC's Management and Administrative Enterprise Database (MAED). The training and education information will be generated within the system.

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

The information is being collected to enable CFTC to track and administer training to its staff and to satisfy regulatory reporting requirements for training.

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

The employment-related information is imported from MAED and is generally collected from CFTC's internal Personnel Clearance System which contains biweekly data updates from the National Finance Center. The training related information is generated as the staff member registers for, and completes training activities.

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

No. While it is a new system, it will take the place of other existing training systems with similar functions and purposes including: Training Log, Training and Events Registration System, and CourseMill.

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

The Government Employees Training Act; 5 U.S. Code § 4103; 5 CFR Part 410; 5 CFR Part 412; Public Law 107 – 347, E-Government Act of 2002; Executive Order 11348- Providing for the further training of Government employees; Executive Order 13111, Using Technology to Improve Training Technologies for Federal Government Employees.

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?

Records for this system will be maintained in accordance with the retention periods in the disposition schedules approved by the National Archives. All approved schedules are available at www.cftc.gov.

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

The training team will adhere to the guidance and policy of the Commission and its Records Office. Data will be purged from the LMS system after the retention period is reached, and any hard copies will be destroyed using Federal agency and CFTC-approved secured practices for disposing of hard copy records.

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)?

Every CFTC staff member will have access to their own records. Access to the records of others will be limited to LMS administrators within the Training Team. Supervisors and business managers will have access only to training data within their teams that includes name, certification, transcript, bargaining unit status, course information, start date, and end date. Contractors who may help in administering the system or training will have access to the information on a need to know basis to perform their duties. FAR clauses related to the Privacy Act are included in CFTC contracts that require contractors to have access to PII.

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

Training data from the LMS will be sent via Secure FTP to the Office of Personnel Management to satisfy monthly reporting requirements for CFTC training activities.

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.

The data will not be released to the public, or any other party except OPM, as required.

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 data is not released publically and there is no known public data set. OPM requires identifiable information to match the training records to existing OPM personnel files maintained for CFTC employees.

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.

CFTC is able to track the disclosure of personal information collected from the LMS by tracing the information back from the external request to the initial collection.

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, and System Managers)?

No other systems share the information or have access to the information generated within the Cornerstone system. Data is imported into the system from internal CFTC systems and exported for internal and external reporting purposes.

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?

Users of the system are presented with a Privacy Act statement the first time they access the system. The Privacy Act statement provides notice to the individuals about the collection, use, sharing, and processing of their personal data. Users will also have continued access to the Privacy Act statement via a link included on the system's main user interface page.

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?

Users voluntarily access the system to participate in training. Notice of the purpose of the collection, use, and storage of the information is presented in a privacy notice when the user initially accesses the system. A user grants consent after reading the notice and proceeding to use the system.

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?

Individuals will have access to their own training records, and any requests for changes to the information can be sent to the LMS administrator. Users will be notified of these procedures by the Training Team, or CFTC Help Desk.

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. Administrative safeguards include agency-wide Rules of Behavior, procedures for safeguarding personally identifiable information, and required annual privacy and security training. 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. Physical 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?

Information retained in the system is visible to the user of the system who can determine if the information is still accurate, relevant, timely, and complete.

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

The system does not provide the capacity to track or monitor the location of an individual in real-time. The system will contain information regarding training approved for an individual, along with the dates and location of the training.

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

Yes, the system complies with all applicable Federal Information Security Management Act (FISMA) requirements. The system is hosted by a 3rd party and is FedRAMP compliant.

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

Users receive annual privacy and security training and must abide by IT Rules of Behavior when accessing systems that contain CFTC information.

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?

Data in the system can and will be retrieved by CFTC Staff name or employee ID.

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 system is covered by CFTC-52, Training Records, CFTC-35, General Information Technology Records, and OPM GOVT-1, General Personnel Records.

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 collection, use, and disclosure of the information in this system have been reviewed by CFTC's Office of General Counsel, and CFTC's Privacy Office and they are consistent with the Commission's Privacy Policy on www.cftc.gov.

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 that the LMS collects more data than is necessary. This risk is mitigated by the Training Team who reviewed the data elements required to properly manage the system and compared those data elements to the data elements mandated by OPM reporting requirements. The LMS does not require certain OPM required data elements, such as SSN, gender, race, and salary information to provide training activities. Therefore, to reduce the amount of PII collected, those elements are not collected by the LMS. The Training Team developed a secure internal process to add the LMS stored data elements to the more sensitive OPM required data elements to ensure CFTC meets its OPM required reporting obligations.

There is a risk for misuse of information by LMS users who have administrative system privileges. All users have role-based access to help prevent users with elevated privileges from accessing information beyond their need to know. The LMS system contains custom reports that can be used to log actions taken by users and administrators. In addition, the CFTC Office of Data and Technology (ODT) performs periodic audits of system log files to ensure access controls are operating as intended. Lastly, all CFTC staff are required to take annual Security and Privacy training.

There is a risk employees are not aware that CFTC is retrieving and using their PII from other internal CFTC systems. This risk is mitigated by appropriate notice from this PIA, the Privacy Act notice that appears the first time a user accesses the system, and the published SORN(s) that cover this IT system.