Privacy Impact Assessment
for
Commission Learning Academy (CLA)

February 2025

Point of Contact

Michael Bartlett

Division of Administration - Human Resources Branch

Reviewing Official

Kellie Cosgrove Riley

Chief Privacy Officer

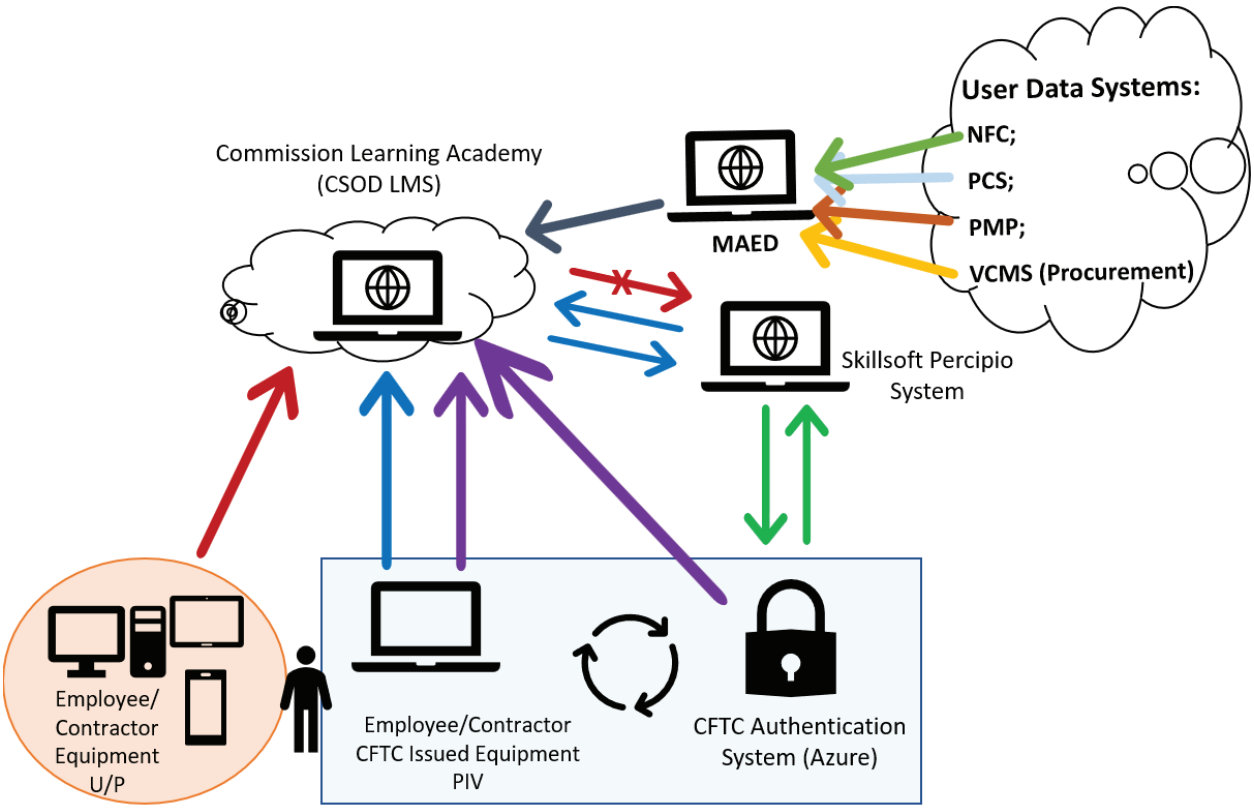
OVERVIEW

The Commission Learning Academy (CLA), a centralized Commercial off-the-shelf (COTS) product from Cornerstone Unified Talent Management Suite (Cornerstone), is the learning management and delivery system for the Commission and its workforce (employees, contractors, consultants, interns, and volunteers). CLA delivers targeted and structured onboarding, compliance, instructor-led, and on-demand training events and courses and provides tracking and reporting of required training data. CLA is managed by the CFTC Human Resources Branch's Learning and Development section and receives technical support through the Division of Administration's (DA) Information and Platform Management section, which manages the interface with the Management and Administrative Enterprise Database (MAED), the main source of information about the CFTC workforce collected and maintained in CLA.

CLA collects general CFTC employment information, as well as training records and related information, about all CFTC staff, including employees, interns, volunteers, and contractors (CFTC users). CLA uses a key field (Employee ID) to identify all CFTC users and transfer their demographic information (name, work email, supervisor, division/office, location and job title) from the various data sets within MAED to CLA. CLA provides compliance reports to internal training stakeholders (complete/not complete) regarding required trainings and to provide overall monthly usage training reports to the Office of Personnel Management. Except for the creation of training titles and associated completion dates in a user's transcript, CLA does not collect, create, or modify personally identifiable information (PII) about the user. The data created and tracked by the CLA is training and transcript status information.

All CFTC personnel use CLA to complete required and discretionary training, while the Human Resources Branch's Learning and Development section manages CLA, and the Data Feeder System Administrator in the DA Information and Platform Management section manages the flow of data to CLA from U.S. Department of Agriculture's National Finance Center (NFC), CFTC's Personnel Clearance System (PCS), CFTC's Performance Management Program (PMP), and CFTC's Vendor and Contract Management System (VCMS) via the Management and Administrative Enterprise Database (MAED) system. On a monthly basis, the Human Resources Branch's Learning and Development section gathers CFTC training data and sends the resulting report to the Office of Personnel Management (OPM), as required by statute.

PII flows to and from CLA as shown below:



The PII data elements collected by CLA are purely associated with a CFTC user's employment. There are only two administrative users for CLA and no individual user has access to another user's CLA data. At the express request of a CLA administrative user for technical service, Cornerstone technical support may gain access to CFTC information in CLA, but the CLA administrative users can withdraw the vendor's access permission immediately at the administrative user's discretion. No other external users have access to CLA.

1. AUTHORITIES AND OTHER REQUIREMENTS

1.1 What legal authority(ies) permit or require the CFTC to collect, use, maintain, or disseminate the information in the system, project, or program?

The following authorities permit the collection, use, and maintenance of PII by CLA:

- 5 U.S.C. § 4103, which empowers the agency head to establish, maintain, and update an agency training program;
- 5 C.F.R. part 410, which imposes agency responsibilities in planning, implementing, evaluating, paying for, and reporting on the agency's training program, and 5 C.F.R. part 412, which provides for training for supervisors, managers, executives, and the Senior Executive Service (SES);
- E-Government Act of 2002, Public Law 107-347, which at Section 209, Federal Information Technology Workforce Development, establishes agency responsibilities in developing and implementing training for federal employees specific to information technology and information resource management; and
- Executive Order (EO) 11348, which provides for further training of Government employees, and EO 13111, which addresses using technology to improve training opportunities for federal government employees.

Collectively, the above laws, regulations, and EOs establish an agency's authority and responsibility to create and operate a training program for the agency's employees, contractors, and other personnel, including the creation, maintenance, and protection of associated records, for the purpose of providing minimum, required training as well as additional, discretionary training for the betterment and professional advancement of the agency's work force.

1.2 Is there a Privacy Act System of Records Notice(s) (SORN(s)) that applies to the information in the system, project, or program? If yes, please identify it. If no, please explain why not.

Yes, the following SORNs apply to records in this system: CFTC-52, Training Records; CFTC-35, General Information Technology Records; and OPM GOVT-1, General Personnel Records.

1.3 Please identify the applicable accreditation boundary evaluated during the Authority to Operate (ATO) process. If the system, or involved project or program, is hosted by a Cloud Service Provider (CSP), please identify the CSP and state whether the system has Federal Risk and Authorization Management Program (FedRAMP) authorization.

The Authority to Operate was issued in May of 2024 for the cloud environment hosting CLA. The Cloud Servicer Provider (CSP) is Cornerstone OnDemand (Cornerstone) and its cloud environment is FedRAMP authorized.

1.4 Is there a records retention schedule(s) approved by the National Archives and Records Administration (NARA) that governs the retention of the records maintained in the system, project, or program? If yes, please identify the schedule. If not, please explain.

Yes. The records in the CLA are subject to CFTC-specific Records Schedule 123, *Employee Training and Professional Development Records*, DAA-0180-2018-0005-0004. These records are destroyed six years after they are superseded or rendered obsolete.

1.5 Please list all forms or other information collection instruments that are used to collect the information in the system. If the information collected is subject to the Paperwork Reduction Act, provide the name of the form or information collection and the applicable OMB control number.

The PRA is not applicable to the information collected in CLA. Most of the information in CLA is collected from an individual's supervisor/manager via CFTC Form 719 when the individual's account is established.

2. INFORMATION

2.1 Identify the information that the system, project, or program collects, maintains, uses, or disseminates.

CLA collects the following data elements for every CFTC employee, contractor, or other personnel currently engaged with the CFTC: name, CFTC email address, pay grade, status, manager or supervisor, division/office, job title, location, CFTC employee ID, and new trainings completed and the completion dates.

2.2 Is the information collected directly from the individual and, if not, what are the sources of information collected. How is the information obtained?

The majority of the information in CLA is not collected directly from the individual. Rather it is obtained from MAED, which receives the information it pushes to CLA from NFC (name, pay grade, status, job title, location, and division/office for non-contractor staff), PCS (email address), PMP (manager or supervisor), and VCMS (information about contractors).

When CFTC users designate new training courses to undertake and then complete those courses, CLA creates entries in that user's record for the training taken and the date completed on a CFTC user's transcript. This is the only information generated by CLA and not obtained from MAED.

2.3 What steps are taken to minimize the collection of information in the system, project, or program?

During procurement of CLA, the CFTC identified the specific data elements required within the system. These data elements were chosen for collection to meet the need to assign and track completion of training requirements, particularly those that are a condition of CFTC employment or other engagement with CFTC.

2.4 Discuss how the accuracy, integrity, and/or quality of the information identified above are determined.

When a CFTC user seeks access to CLA via a CFTC device and enters their email address, CFTC's Single Sign-On (SSO) automatically reviews the entered email address and compares that email address to the records in CFTC's Entra ID (Active Directory) to confirm that the email address is accurate before access to CLA is granted. CLA relies on the sources of the PII it collects via MAED to determine the accuracy, integrity, and/or quality of that PII.

Every quarter, the CLA administrator reviews the user list, including the associated supervisory information, in CLA to ensure it remains accurate. If any changes are needed, the administrator sends a request to the CFTC helpdesk to have the information updated or otherwise corrected.

In the event there is an error in a user's transcript associated with the training taken or date of completion, the CFTC CLA administrator would make a note in the transcript to identify the needed edit and then work with CLA to correct the edit. The CFTC user would have to identify any errors and inform the CLA administrator user of the need for a correction or update of transcript information.

2.5 Privacy Impact Analysis: Related to the Collection and Characterization of the Information

With the exception of the title of assigned training courses and completion dates for completed trainings, all of the PII in CLA comes from trusted outside sources via MAED. In addition, if an individual finds an error in their training record, the CLA administrator can correct it with CLA. Accordingly, there is a low risk to the individual that inaccurate information could result in adverse consequences.

3. USE OF THE INFORMATION

3.1 Describe how the information is used internally at the CFTC to support a business purpose.

The PII collected by CLA is used to (1) track and confirm that CFTC employees, contractors, and other personnel have completed required training, which is a condition of employment/engagement with CFTC , as well as voluntary or optional training; and (2) provide reports on training of CFTC personnel to the Office of Personnel Management (OPM), as required by and described in 5 C.F.R. Part 410 – Training. These uses are consistent with the laws identified and described in response to Question 1.1, above and the purpose of CLA's collection of information is compliance with those laws.

3.2 Identify all programs or offices, and an approximate number of individuals, within the CFTC that have assigned roles and responsibilities with respect to the system, project, or program or with whom information is shared. Explain how each uses the information.

Because training is mandatory and a condition of continued engagement with CFTC, all CFTC personnel, including employees, contractors, consultants, interns, and volunteers, across all Offices/Divisions (totaling approximately 1,141 individuals) will be users of and have an account with CLA. With the exception of CFTC's CLA system administrator and separate technical administrator, all other users have default user accounts and will not be able to access any other individual's PII other than their own. There is also a limited number of users that have elevated CLA privileges for specific actions, e.g., SF-182 training requests and mandatory compliance training reports. The two CFTC administrators are responsible for ensuring the accuracy of current user lists, arranging for new and existing trainings available in CLA, addressing any technical issues (and engaging Cornerstone for that purpose, to the extent needed), generating training-related reports, and ensuring the smooth operation of CLA. In addition, employees and contractors in the enterprise security operations center (eSOC) require access to address any security-related issue or investigation associated with such an issue.

3.3 Privacy Impact Analysis: Related to the Internal Access and Use

CLA has been configured such that only those persons with an official need for access to CLA accounts and the PII therein in fact have access to CLA accounts. All access requests and related decisions are sent to the administrator for acceptance and implementation or denial. The administrator can run six separate reports to audit the use of and any changes to data in CLA; and can quickly update or revoke a user's access in the event, e.g., an improper change to CLA data is made. The administrator also works with Cornerstone to correct or update any data including PII upon notice that it has been improperly changed or rendered incorrect or outdated. In addition, CLA tracks and records any changes to the information in CLA, enabling any improperly changed data to be identified and corrected as needed. Accordingly, the risk associated with unauthorized internal CFTC access to the data appears be low and any impact accordingly appears to be minimal and quickly correctible.

4. INFORMATION SHARING

4.1 Is the information shared outside of the CFTC as part of usual agency operations? If so, identify the organizations or individuals with whom the information is shared, how and why it is shared, and how it is to be used.

Yes. Pursuant to 5 C.F.R. Part 410 – Training, the CFTC sends a monthly training report to OPM that includes the CLA user ID, i.e., the CFTC employee ID, and all training completed by that employee. To convey each report, the CLA administrator puts the CLA data into a comma-separated value (CSV) database, which includes user IDs but not names, and uploads the resulting file into a file transfer protocol (FTP) site. CFTC's Division of Administration – Information Technology (DA-IT) then sends the file/report to OPM's enterprise human resource, which is also known as the EHRI database, by uploading the file/report to OPM's online portal.

Information in CLA is also shared with the contractor so that any needed technical assistance can be provided.

4.2 How is the information sharing described in 4.1 compatible with the purpose for which it was originally collected described in 3.1?

Sharing of the information in CLA with the contractor, when necessary, ensures the continued, proper functioning of CLA and sharing the training-related information with OPM is required by 5 C.F.R. Part 410 – Training. Both of these disclosures are made pursuant to an applicable routine use and are compatible with the purpose stated in CFTC-52, to provide CFTC with a means to track training registrations, scheduling, scores, completions, and other training metrics to assess the effectiveness of training, identify patterns, respond to requests for information related to training of CFTC personnel and other individuals, and facilitate the compilation of statistical information about training.

4.3 Is the information sharing documented in a Memorandum of Understanding, other information sharing agreement, or a contract?

There is no MOU or other sharing agreement with OPM that references the sharing of the training information, but the records are co-owned by OPM as are all general personnel records and OPM is subject to the Privacy Act and other Federal privacy laws and guidance.

There is a contract pursuant to which the CFTC acquired the CLA via Cornerstone and it is pursuant to that contract that the CFTC permits the CLA contractor to access information in the system when necessary for the contractor staff to provide technical assistance.

4.4 Are there limitations on re-dissemination of the information by the third party in place, either in the documents identified in 4.2 or otherwise?

There is no explicit prohibition on re-dissemination of the records that are provided to OPM is accordance with the CFTC's legal and regulatory requirements. However, OPM co-owns those records and has the same Privacy Act and other Federal privacy requirements as the CFTC.

Likewise, when the CFTC provides access to the contractor staff in order to obtain technical assistance, as a terms of the contract they are required to access and handle CFTC's records in accordance with the Privacy Act, which provides that agencies externally share any records from a system of records only as permitted by the applicable routine uses.

4.5 Describe how the system, project, or program accounts for and maintains a record of disclosures outside of the CFTC.

Information, including PII, retained by CLA is generally shared internally to those employees and contractors with a need-to-know, pursuant to 5 U.S.C. 552a(b)(1), which is an exception to the accounting of disclosures requirement. For those other instances where CLA PII is shared to external persons or entities, as described in the routine uses identified in the applicable SORNs, a process has been constructed to comply with the Privacy Act requirement for retaining an accounting of disclosures, whereby for any instance of required disclosure of PII from CLA to any external person, agency, or entity, CFTC will transcribe on a dedicated spreadsheet the date, nature, and purpose for sharing the PII and the name and address of the external person, agency, or other entity to whom the PII will be/is disclosed.

4.6 Privacy Impact Analysis: Related to Information Sharing

The training reports provided to OPM are limited to the information required by applicable law and regulation, and the CFTC administrator for CLA only includes user IDs and does not include any names or other PII in the transfer of the file/report to OPM. DA-IT uploads the file/report, which is created and directly provided by the CFTC administrator for CLA, to OPM via that agency's dedicated online portal. CFTC also controls all vendor access to CLA PII by expressly granting access that is limited to what is necessary, in order to address a technical issue involving CLA or its data, and CLA can revoke that access at will and at any time. Based on the above, there appears to be a low risk that any information provided could be altered or omitted/deleted during this transfer.

If PII from CLA were to be compromised, affected CFTC users risk the exposure of their CFTC/business-related contact information but not any of their personal information. Any impact would likely be experienced in the accuracy of a CFTC's user's training-related data, which due to the fact that training is a condition of

continued engagement with CFTC, could affect that user's perceived compliance with training requirements and accordingly that user's continued engagement with CFTC. As noted above, the CFTC administrator for CLA can directly change incorrect or manipulated data to render it accurate and complete, as needed.

5. DATA RETENTION

5.1 Explain how long and for what reason the information is retained.

Records created by CLA are retained for six years after those records are superseded or rendered obsolete, at which time those records are destroyed in accordance with the records retention schedule identified in Section 1.4.

CLA records dated before 2019 were moved to an online archive and are not maintained by CLA. Those records along with numerous other archived records of the Human Resources Branch (HRB) were sent to Iron Mountain for mass destruction and Iron Mountain in fact destroyed all such documents in June 2024. The remaining CLA records will be destroyed as they reach the applicable 6-year disposition date.

5.2 Describe how the information is disposed of at the end of its retention period.

When a CFTC user ends engagement with CFTC, the corresponding CLA account is rendered inactive and inaccessible to everyone except for the CFTC administrator for CLA.

CFTC recently acquired functionality within CLA that will permit two options for addressing the retention of information within the system: anonymization and/or deletion.

The CFTC administrator is still investigating this newly acquired functionality and no decision has yet been made on how to proceed.

5.3 Privacy Impact Analysis: Related to Retention

Although no CLA records have yet been retained for the period described in the applicable records schedule, the schedule for anonymization or destruction of CLA user records continues to be considered and has not yet been determined or otherwise implemented with Cornerstone. Once CFTC has made the decision and accordingly established the preferred anonymization or deletion method, as described in the response to Question 5.2, CLA will automatically anonymize or delete data at an interval tracking the applicable record retention requirements.

Based on the current state of record deletion capability, Cornerstone potentially maintains inactive user accounts indefinitely. However, Cornerstone is not able to access client data unless and until a client expressly requests Cornerstone to do so and creates/enables a Cornerstone account in the client instance of CLA. Once the client grants and provides access, the client can revoke that access at any time. Accordingly, it appears to be a low risk associated with data retention and that risk will be further mitigated once CFTC has made a decision regarding the anonymization and/or deletion of PII and that resulting process has been implemented.

6. NOTICE

6.1 How are individuals provided notice prior to the collection of their information? If they are not provided notice, please explain why.

When a user logs into the CLA site and enters their email address to authenticate against that user's credentials via CFTC's Single Sign-On (SSO), the user is presented with a Privacy Act Statement (PAS) and must engage the "ok" button to remove it and gain access to the CLA website. The PAS provides the authority for, purpose of, intended uses of, applicable routine uses of, and consequences for declining to provide the information being collected by CLA.

In addition, more generally, a PAS describing, e.g., the authority and intended use of the data collected is attached to the SF-182, which is completed by all CFTC employees, contractors, and other personnel when they request to take training. That PAS provides the authority for, purpose of, intended uses of, applicable routine uses of, and consequences for declining to provide the information being collected. CFTC employees, contractors, and other personnel who use CLA are also provided with notice about the collection of their PII via the CFTC-52, Training Records, CFTC-35, General Information Technology Records, and OPM/GOVT-1, General Personnel Records, SORNs which identify the authority for, purposes of, and administrative/technical/physical safeguards for the information collected.

6.2 Do individuals have the opportunity to consent to the use of their information or decline to provide their information? Please explain.

There is no opportunity for users to consent to CLA's collection of their PII. CLA's collection of PII is required for CFTC to discharge their statutory and regulatory obligation surrounding training of its personnel and related reporting requirements.

6.3 Privacy Impact Analysis: Related to Notice

CFTC users receive notice of the collection of their data via the Privacy Act statements and SORNs identified and described in Section 6.1, but the collection of

this data is a condition of initiating and continuing engagement with CFTC. If users refuse any portion of that collection, they will not be permitted access to the CFTC network, will not be able to discharge their assigned work responsibilities, and will soon thereafter be removed from engagement with CFTC. The cited PAS and SORNs mitigate the risk associated with notice but do not completely remove that risk, since much of the PII collected by CLA originates from the four systems identified above and not directly from individuals. Individuals do not have the opportunity consent or object to any particular use of their PII. Individuals' PII collected by CLA, which PII consists entirely of CFTC employment related information, is used only for monitoring and reporting on employees' training, including required and discretionary training. Accordingly, the risk associated with notice, although technically not actionable due to the mandatory nature of the collection, appears to be low.

7. REDRESS

7.1 What procedures are in place that allow individuals to access their information?

Individuals may view their active, complete, and archived training transcripts, as well as their user record showing name, division/office, job title, email address, and location, among other information, online and may save a copy of their transcripts, all within the CLA site.

In addition, a Privacy Act request can be made by individuals to gain access to their data held by this information system, pursuant to the directions provided in 17 C.F.R. § 146.3 - Requests by an individual for information or access, as stated in CFTC-52, Training Records (83 FR 23433) (May 21, 2018) and OPM- GOV'T 1 General Personnel Records. A person must submit a written, signed request that includes the full name of the person seeking the records, that person's home and business addresses and telephone numbers, and the title and number of the SORN covering the records sought.

7.2 What procedures are in place to allow individuals to correct/amend inaccurate or irrelevant information about themselves?

Users may contact the CFTC CLA administrator to request an update to their information in CLA. The CLA administrator then contacts the Data Feeder System Administrator to request the update of the information being pushed from other sources, i.e., NFC, PSS, PMP, and VCMS, via MAED.

In addition, a Privacy Act request can be made by individuals to correct or amend their data held by this information system, pursuant to the directions provided in 17 C.F.R. § 146.8 – Amendment of a record, as stated in CFTC-52, Training Records (83 FR 23433) (May 21, 2018, and OPM-GOV'T 1 General Personnel Records. A person must submit a written, signed request that describes the records in need of

amendment and specifies the amendment sought and the basis for the requested amendment. CFTC will promptly determine whether to grant the request and either make the amendment requested or inform the person of the reason for denying the request and provide the procedures for administrative review of the CFTC's denial.

7.3 How are individuals notified about the procedures for correcting/amending their information?

CFTC personnel are provided with instructions during CLA-related training on how to work with the CFTC administrator for CLA to update or correct their PII in the system. In addition, the applicable SORNs and the CFTC's Privacy Act regulation describe the general process to seek a correction or amendment of information collected by CLA.

7.4 Privacy Impact Analysis: Related to Redress

CFTC users have the ability to access their own CLA user records and transcript and to identify any needed corrections or amendments and can arrange for any correction or amendment of their data with the CLA administrator. Accordingly, individuals' risk of not having the opportunity to learn and seek correction or amendment of their PII is low.

8. AUDITING AND ACCOUNTABILITY

8.1 How is the information in the system secured?

For CFTC users, information is secured by assigned security account roles (default user and administrator); and account/system access requires a username and password when using a non-CFTC device, or Single Sign-On (SSO) when accessing CLA via the CFTC network.

The majority of the technical safeguards, including but not limited to firewalls, are inherited by CFTC from Cornerstone, as provided in the FedRAMP Control Responsibility Matrix (CRM) Worksheet for CLA. However, CFTC users must either use a CFTC device and PIV or a CLA username and password and be registered in CFTC's Active Directory (AD) to access CFTC's instance of CLA. Contractors working at or for CFTC are required to sign a non-disclosure agreement (NDA) as a prerequisite to accessing the CFTC network or seeing any CFTC non-public or otherwise sensitive information. When accessing CLA from a CFTC device, the user must engage the CFTC Virtual Private Network (VPN) to sign onto the CFTC network and from there to CFTC's instance of CLA. CLA passwords are only viable for 60 days, regardless of (in)frequency of use, after which a CFTC user must request a new password or reset the existing password, both of which actions require access to the user's CFTC email to complete. CLA is currently in the process of employing multi-factor authentication (MFA).

Regarding administrative safeguards, CFTC, like all Cornerstone clients, has its own CLA database instance within the Cornerstone environment that contains all of CFTC's information. Other clients cannot access or view CFTC's database information, or vice versa, within the Cornerstone environment. All Cornerstone personnel must sign and conform to the CFTC Rules of Behavior to be granted access to the CFTC network. There currently is no requirement for Cornerstone personnel to individually sign a non-disclosure agreement (NDA). There are separate CLA manuals covering general and administrative access, respectively, and training is available that covers the contents of those manuals. CFTC also has the capability to create, modify, and disable temporary and emergency accounts for Cornerstone. Cornerstone maintains audit trail information for the creation, modification, or disablement of accounts, which information is maintained in the modification history for the accounts. Cornerstone uses security roles to grant and restrict access and by default users are not provided a role until assigned by a CFTC administrator for CLA.

CFTC's continuous monitoring program includes CLA.

8.2 Are audit logs generated reflecting access and use of the information in the system? If not, please explain. If so, please describe how often they are reviewed and for what purpose.

Yes, CFTC's CLA administrator can use CLA to generate multiple audit logs reflecting access and use of the information system. The audit reports include a "Security Role Audit Report", "Login Report", "Security Role User Permission Report", "Proxy as User Report", "Security Role Report", and "User Record Audit Report", each of which contains various date elements.
These audit logs can be run by the CLA administrator at any time. Currently, there is no scheduled for the production or review of the above reports.

8.3. What procedures are in place to determine who has access to the system, and are they documented?

Since training is a requirement for initiating and continuing engagement with CFTC, whether as an employee, contractor, or other personnel, all CFTC personnel identified in CFTC's Active Directory (AD) are provided access to CLA for training purposes. Only two CFTC employees have been assigned administrative access to CLA for purposes of discharging CFTC's responsibilities in operating and maintaining the information system. This role-based access is based on need-to-know and is determined and approved by the Chief Human Capital Officer.

The CLA administrator creates an account for all users once they have been onboarded to CFTC and established in CFTC's AD. Cornerstone is responsible for assigning permissions to user accounts to meet the CFTC's security policy. CFTC bears the responsibility of establishing a "separation of duties" for its workforce using CLA.

CFTC's review of each user role (built-in or custom) is restricted to only those functions and permissions that are required to fulfill users' duties. Users are also assigned group memberships to ensure they can only access their CFTC data.

CFTC creates, monitors, and disables temporary and emergency accounts created for Cornerstone (primarily to provide technical assistance in response to a specific CFTC request). All Cornerstone employees with access to CLA have undergone background checks authorizing them to access Federal Government client data.

8.4 Describe what privacy training is provided to users, either general or specific to this system or project.

Completion of initial and thereafter annual security and privacy awareness training is a prerequisite to a user gaining and maintaining access to the CFTC network. All users must sign the CFTC Information Technology Rules of Behavior Acknowledgment, which memorializes this requirement.

The requirement to complete security and privacy awareness training is immediately charged to an employee or contractor upon onboarding to CFTC, i.e., after their AD account is created, and must be completed within two days. If the training has not been completed in the two-day period, the user's AD account is automatically disabled, preventing that user from accessing the CFTC network to any degree, and the account remains disabled until the training has been completed.

8.5 Privacy Impact Analysis: Related to Auditing and Accountability

Only the two CFTC administrators for CLA, as well as members of CFTC's eSOC in the event a security issue or associated investigation requires access to CLA, have a need to know and accordingly can access the six reports described in the response to Question 8.2 above. Currently, there is no defined schedule for creating or reviewing any of the six CLA reports that can be generated by the CFTC administrator. In the event one or more reports abnormal or potentially suspicious or malicious activity, the CFTC administrator would follow the procedures described in CFTC Policy: Responding to Incidents Involving CFTC Confidential Information and immediately notify the CFTC Incident Response Team. The absence of an establish schedule for producing and reviewing the available CLA reports covering access, data modification, and all other activity within CLA creates a privacy risk regarding audits, but the risk appears to be low.