EXHIBIT K

Attach as Exhibit K a description of the measures or procedures employed by registrant to provide for the security of any system which performs the functions of a clearing agency. Include a general description of any operational safeguards designed to prevent unauthorized access to the system (including unauthorized input or retrieval of information for which the primary record source is not hard copy). Identify any instances within the past year in which the described security measures or safeguards failed to prevent unauthorized access to the system and describe any measures taken to prevent a recurrence of any such incident. Describe also any measures used to verify the accuracy of information received or disseminated by the system.

A. Background Measures and Procedures Relating to Systems Security Employed by the Applicant

The Applicant employs various measures and procedures to provide for the security of systems used when performing the Client Services set forth in Exhibit J. The systems utilized in providing the Client Services set forth in Exhibit J are owned by DTCC and provided to the Applicant pursuant to the Services Agreements. The Applicant's controls with respect to the Client Services consist of Information Security and IT Risk Management Controls implemented by DTCC via the Services Agreements.

B. Regulation SCI ("Reg SCI") and Applicability to the Applicant

If the Applicant is approved as an exempt clearing agency, it will become an "SCI Entity," subject to the Reg SCI policies and procedures implemented by DTCC, as set forth herein. DTCC performs functions for the Applicant to comply with Reg SCI obligations pursuant to the Services Agreements. The enterprise-wide measures and procedures applicable to entities within DTCC subject to Reg SCI are below.

C. DTCC Enterprise-Wide Measures and Procedures Relating to Reg SCI

The Applicant will be subject to various DTCC measures and procedures at the enterprise-wide level which, together, comprise the program for compliance with Reg SCI for DTCC subsidiaries, which are defined as "SCI Entities." In accordance with Rule 1001, DTCC maintains written policies and procedures reasonably designed to ensure that its SCI systems and, for purposes of security standards, indirect SCI systems, have levels of capacity, integrity, resiliency, availability, and security, adequate to maintain DTCC's operational capability and promote the maintenance of fair and orderly markets. DTCC's written policies and procedures also address the Applicant's obligations to take corrective action and provide notice to the SEC and others of SCI events in accordance with Rule 1002. Various technology processes and controls comprise DTCC's compliance framework for Reg SCI and are subject to annual review and assessment pursuant to Rule 1003. The annual Reg SCI review for the Applicant will cover: business continuity, capacity planning, change and release management, disaster recovery, governance and compliance, incident and problem management, logical security, penetration testing, physical security, security incident management, stress testing, system development lifecycle, technology testing, and vulnerability management. Business continuity and disaster recovery testing is conducted pursuant to standards

developed in accordance with the requirements of Rule 1004, and records relating to Reg SCI are kept pursuant to Rule 1005.

D. DTCC Enterprise-Wide Information Security and IT Risk Management Controls

The Applicant is subject to the DTCC Corporate Risk Management Policy, an enterprise-wide policy that establishes the DTCC Corporate Risk Framework. As set forth in Exhibit J, DTCC's Corporate Risk Framework is applicable to DTCC's subsidiaries, including the Applicant, and defines the risk management program applicable to DTCC and its subsidiaries.

E. The Applicant's Systems Safeguards Are Implemented by DTCC

The Applicant's cybersecurity safeguards are implemented as a shared service which the Applicant receives from DTCC and various affiliates pursuant to the Services Agreements. These policies and standards, which are established by DTCC's Cybersecurity Risk Office ("CSRO") & IT are in alignment with an industry-accepted risk management framework.

DTCC's Chief Information Security Officer ("CISO") is situated within DTCC's first line of defense and fully embedded with IT operations and day-to-day security management. Within the second line, the Chief Cyber Security Risk Officer ("CCSRO") focuses on independent challenge of control coverage and effectiveness, risk management enhancements and supporting a proactive cyber security posture. In addition, DTCC's Head of Business Continuity & Resilience ("BCR") reports to the CRO. Both the CISO and Head of DTCC BCR facilitate DTCC's ability to monitor and mitigate risk, build new capabilities, unify IT cybersecurity functions, and strengthen the resilience of DTCC and its subsidiaries, including the Applicant.

DTCC supports the data security and technology risk requirements of the Applicant pursuant to the Services Agreements. DTCC implements and manages information security and risk management processes that identify information security threats, measure information and technology risks, and protect the information from these risks for all DTCC subsidiaries, including the Applicant. DTCC identifies and communicates control gaps to the Applicant's management and reduces the overall exposure of DTCC and its subsidiaries to information and technology risks.

Risks are evaluated, communicated, and escalated through the enterprise through DTCC Management Risk Committee and the DTCC Board Risk Committee, as described in Exhibit A.

The primary CSRO and IT programs are outlined below, followed by a table that sets forth the application of these programs to the Client Services set forth in Exhibit J.

1. Cyber Threat Intelligence

The primary objective of DTCC's threat intelligence program is to gather information from public and private sources to glean a picture of the cyber threat landscape and any significant changes to the tactics, techniques, and procedures of threat actors in order to extract insights into potential current and future attack vectors. Threat intelligence is collected from several external sources including trusted intelligence providers, public and private sector agencies and partners, National Computer Incident Response Teams, and collaborative threat intelligence working groups. The threat intelligence program endeavors to provide relevant, actionable intelligence and may require

DTCC to evaluate its processes and technology-based controls and implement countermeasures, if necessary, to limit the exposure to a threat.

2. *Insider Risk Program*

The mission of the Insider Risk Program ("IRP") is to mitigate the risk from insiders, both malicious and accidental. The IRP takes into consideration DTCC's culture, tolerance for risk, and the privacy of its employees. The primary directives of the IRP have been designed around these core values and certain best practice recommendations.

The IRP has three primary directives: (1) the protection of sensitive (confidential or restricted) data, (2) the identification of potential tampering with critical databases, and (3) the identification of individuals who may pose a heightened security risk to DTCC and its subsidiaries, including the Applicant. These program directives capture the scope of threats that the IRP is currently focused on. The underlying motivation for these types of threats is supported by the IRP's directive to attempt to identify individuals who may pose a heightened risk.

3. *Network-based Penetration Testing and Threat Hunting*

The Offensive Cyber Security team is responsible for performing network-based penetration assessments and cyber threat hunting. Network-based penetration assessments are designed to simulate real world threat actors and methodologies and are performed with the assistance of trusted third parties. Testing is conducted around specific scopes of assets, network segments, specialized environments, and security controls. Both external and internal assessments are conducted. External security assessments are conducted from outside the organization's security perimeter offering the ability to view the environment's security posture as it appears outside to real world threat actors. For internal security assessments, assessors work from the internal network and assume the identity of a trusted insider or simulating an attacker who has penetrated the perimeter defenses to reveal weaknesses that could be exploited. Internal security assessments also focus on system-level security and configurations to include application hosting, service configuration, authentication, access control, and system hardening.

Cyber threat hunting is a proactive cybersecurity practice that involves actively searching through networks, systems, and data to identify and mitigate threats that may have evaded existing security measures and controls. Long-term and short-term threat hunts are performed in addition to recurring operational threat hunts. Long-term threat hunts are conducted based on a prioritized "back log" list of hypotheses of potential threats. Short-term threat hunts are shorter in duration utilizing information received such as cyber threat intelligence and vulnerability notification data as well as to determine if a long-term threat hunt is necessary. Operational hunts are recurring short-term hunts providing oversight on other security controls and functions including network perimeter monitoring, attack surface management, potential exposed passwords, etc.

4. *Vulnerability Management Oversight Program*

The Vulnerability Management team is responsible for the vulnerability management oversight program which monitors vulnerability detections and remediation efforts providing weekly and monthly reporting of key risk and performance metrics, it also provides tracking of escalated

vulnerabilities that are deemed critical or emergency in nature that would cause significant impact to DTCC. In order to effectively identify weaknesses in the DTCC environment, the team uses software scanners to identify vulnerabilities.

Once the software vulnerabilities have been identified, DTCC classifies the weaknesses, factoring location of the vulnerability within the computing environment (e.g., internal vs. external network), ease of vulnerability exploitation, business impact of the software weakness and the presence of other organizational processes and technical safeguards. The classification of software weaknesses dictates the remediation schedule. Remediation may require the application of a software patch, a newer version of the software, or the application of compensating controls.

5. *Ethical Application Penetration Testing ("EAPT")*

Ethical Application Penetration Testing uses simulated real-world attack scenarios to identify exploitable vulnerabilities in an application. Penetration testing helps determine how well the system withstands threat actor attack patterns and the level of sophistication required by an attacker to compromise an application. It also provides information on additional countermeasures, as needed, to mitigate threats against the system. DTCC utilizes experienced risk assessors to perform these tests.

The DTCC business web applications and APIs are subjected to the EAPT in the QA environment or as needed in the Production / Production Support Environment. All business web applications and APIs (including DTCC-hosted, third-party-hosted, and cloud-hosted) accessed by the Applicant's Clients are in scope for application penetration test selection, as set forth in Table 1 below.

As part of EAPT, DTCC designated testing personnel will:

- Run automated dynamic scans and manual tests on DTCC and third-party (external from the Applicant and its affiliates) web applications and APIs.

- Publish the results of application Pen Test along with the finding details.

6. *Security Design Oversight*

The Cyber Security Standards and Design Oversight team ("CSSDO") performs detailed reviews of all security aspects of an information system design. These reviews are based on a set of requirements developed by the information security organization and guide system design. Security architecture includes, but is not limited to, network segregation, security baselines, authentication mechanisms logging, monitoring, encryption, and data classification.

Network segregation allows for systems with different security requirements and/or operational environments to be physically or logically separated from other information systems on the network. Network segmentation provides an additional security benefit of network isolation, which may be used in troubleshooting or, in the event of an incident, may be used to limit the exposure to certain network segments. Network boundaries are implemented using routers, firewalls, and/or gateways.

Security baselines are a set of specific security configurations for a technology that are designed to limit the exposure of the system to cyber threats. Security baselines are set by a combination of DTCC's CSSDO, security architecture, and IT groups. In order to ensure that these minimum controls are always set, the DTCC IT organization, together with CSSDO, creates a secure build (i.e., a process designed to consistently apply certain security controls to an information system upon installation). Security baselines may differ based on where the information system resides on the organization's network (e.g., internal, internet facing).

All systems are configured using security baselines specific to the operating system and/or applications. Security baselines are based upon industry, vendor, and regulatory best practices. Baselines are updated at least annually. The security attributes of these baseline configurations are measured by an automated system to identify any defects. Any defects identified are tracked to resolution.

Authentication mechanisms are used to validate users of the information system. Authentication may use multiple factors. Authentication methods are selected based on the information and services that are provided.

7. *Identity and Access Management ("IAM")*

IAM manages the process of limiting access to authorized users based on what is required for their job responsibilities. IAM is also responsible for ensuring user access is recertified and reviewed by a user's management from the time of access creation to the point when access is no longer required. Key activities for IAM include account creation, user transfer certification, periodic user certification, and user termination. This service also includes the management of privileged access and shared accounts used to access information systems. Application of this service to these accounts provides accountability to their usage and records the rationale for their use. Role-based access brings together groups of individuals with similar access needs and provides access permissions to the user group. Role-based access mitigates the risk of overprovisioning user access. Role-based access control also provides consistency in the provisioning of access to business groups.

Individuals with access to the Client Services require explicit approval prior to obtaining access.

8. *DTCC Intrusion Protection Management*

Intrusion Protection Management is comprised of system tools and processes used to detect unauthorized access to an information system. Information systems used to identify intrusions include, but are not limited to, network-/host-based intrusion detection and protection systems and network-/host- based anti-virus/anti-malware intrusion detection systems.

Host-based intrusion detection systems are software-based solutions that reside on the information system for which monitoring is being applied. Network-based intrusion detection systems are hardware-based solutions that sit in the line of network traffic to monitor for anomalous or malicious activity.

During the last year, there were no cybersecurity intrusions or targeted threats that related to the Applicant or its systems.

9. *Risk Assessments*

DTCC executes a risk assessment service, which provides risk identification and advisory services to DTCC and DTCC subsidiaries including the Applicant. The service includes risk assessments of applications, infrastructure, IT Processes, and regulatory related assessments. The key components include assessment scope, assessment against a defined framework (e.g., Process Risk Control library), control findings identification, confirmation, and reporting. Risk assessments are completed through a facilitated approach with the objective of providing reasonable assurance that the "target of evaluation" and its related administrative processes are meeting or exceeding organization information security standards.

10. *Security Awareness, Training and Education*

DTCC has a dedicated team for Security Awareness Training, Education and Communication ("SATEC"). They provide a robust security awareness program for all DTCC staff, including the Applicant's personnel.

Security awareness is used to inform the organization and its users of the desired security behavior. Communication is conducted through email distribution, workshops, posters, corporate websites, and other communication vehicles. Security training is used to measure (i.e., test) the effectiveness of security awareness communications. This is accomplished through mandatory e-learning with scored testing (e.g., security modules, interactive phishing exercises). Role-based security education provides a more specialized security training that is centered on a specific or specialized skill set (e.g., secure coding).

The content of the DTCC programs is driven by current and emerging threats, new regulatory/supervisory rules, and changes to the organization's perceived threats. Given the heightened threat of phishing attacks, regular simulated phishing campaigns are a key part of the program. These are reinforced with monthly phishing lure and cybersecurity awareness tips newsletters and ongoing communications that enforce the safeguarding of information and heightened awareness of social engineering tactics.

F. Other Internal Controls (SOC 1, Type II Controls)

Certain of the Applicant's controls will be subject to a SOC I, Type II audit, as described in Item 6(b) of Schedule A of Form CA-1. These additional control objectives include logical access controls, balancing controls, physical access, change management, job scheduling, and data archive/retention. These control objectives are set forth in more detail below.

1. Client New Entity Record Setup

Client New Entity Record Setup

Agreements for the setup of new Client entities onto Client Services are approved by the DTCC Client Account Services team ("CAS"), whose function is to review, approve, and store the final contract in a document repository. The CAS Team facilitates the setup and maintenance of user records. An automated workflow tool is used to document and track the steps in the onboarding process for new Client Services. New Clients are set up in PNO (as defined in Exhibit N) after approval has been obtained from appropriate internal stakeholders for CTM, ALERT, TradeSuite ID, and Settlement Instruction Manager.

TradeSuite ID uses the TradeSuite ID Masterfile to manage the unique user identifier that is assigned to a Client organization subscribing to TradeSuite ID. This unique identifier is used to identify and validate data from Client organizations and is also used as a means to restrict each Client's access to its own data. Updates to master data are authorized by the Client and independently reviewed prior to processing. A quality review is completed for a sample of master data changes to ensure that each change was processed accurately and completely.

In the future, there will also be functionality available for non-self-affirming institutions (as described in Exhibit J) that wish to obtain a TradeSuite ID (referred to as the "ID Only" set-up and referenced in Exhibit J). Controls will need to be determined and tested at a future date, based on the TradeSuite ID user set-up established for these non-Clients (these entities will not have MSAs, as set forth in Exhibit P, and will not have any access to TradeSuite ID systems).

Client Lifecycle Setup and Maintenance

The CAS Team assists the Client in the management of Client user access to the Client Services. Upon executing the relevant documentation provided in Exhibit P the access request process begins with a written request, submitted by authorized Client personnel. This request may be received via mail, email, or electronic online forms from MyDTCC. For Client user access, the Client product administrator can fully maintain Client user profiles via secure login to MyDTCC with changes processed automatically.

Client user accounts (also referred to as access authorizations) in PNO are synchronized on a real-time basis with the authentication tool for Client Services. Initial Client user account passwords are systematically generated upon Client user account setup and are systematically enforced to be changed at initial user login. User password resets are requested by the Client through an authentication process. Identity verification procedures are performed prior to disclosing a new password to an authenticated user. Clients can reset their own passwords. User IDs and passwords, whether new or resets, are distributed to users through their user product administrators

via a secure log in to MyDTCC or via telephone. Identity verification procedures are in place to ensure that system login information, such as login ID and initial password, is disclosed to the appropriate individual. Upon creation of a new Client user account, a number of access rights are automatically granted to the account based on the Client entity subscription(s) and potential relationships between existing Client entities. Clients are responsible for their own password management.

User passwords require a minimum length and password complexity. User passwords expire after a pre-determined number of days and are locked after a pre-defined number of failed attempts.

2. Data Center Access

Physical access to the data centers is regulated through restrictive security measures using a combination of strategically positioned interior and exterior surveillance video cameras and a badge access system with two-factor access control. For authorized access into the computer rooms, a detailed event request must be submitted and approved.

The data center access list undergoes recertification/review semiannually by the owner of Data Center Access. Upon an employee's termination, all data center access is promptly revoked.

Data center buildings are equipped with dedicated security officers within the security operations center. [redacted]

All employees and visitors entering the data center must have received prior authorization from DTCC Data Center Operations. [redacted] To guarantee safety and security, visitors are always escorted by an authorized DTCC Data Center Operations or Global Security Management staff members.

The security camera network records real-time digital video. Cameras are strategically positioned to monitor critical areas, and several video monitors in the security operations center are dedicated to real-time monitoring of the data center facility.

3. Change Management and Emergency Changes

The purpose of the operations change management process is to facilitate the scheduling and coordination of changes to production environments. This process controls modifications to hardware, software, networks, infrastructure, and documentation to ensure that the Applicant is

protected against improper or unauthorized change activity and to ensure that changes are enabled with minimum disruption to products and services.

Automated formal notification is received, reviewed, and authorized before a change is made. Changes are installed in development, QA and/or Client test environments as needed before they are deployed to production. The install plan and rollback plan must be tested in QA and/or Client test before any major release.

The production environments are appropriately segregated from non-production environments. The function to migrate the Applicant's application source code to the production environment is limited to appropriate personnel. Database access is recertified semiannually, and access modifications requested as a result of the review are implemented timely.

4. Production Environment Monitoring & Support

Escalations regarding application support are initiated by DTCC's Technology Operations. Additional notifications can occur via alarms generated by the applications. Once DTCC Technology Operations is notified of a problem, it validates that the issue lies within its applications and determines the root cause. The DTCC Technology Operations team can then fix the problem and confirm if no action is needed, or further escalate to the Applicant's management for additional research and possibly initiate a task force. If changes are needed, modifications must follow the emergency control procedures utilizing the workflow tool. DTCC Technology Operations is kept informed of all actions inclusive of no actions; any necessary restarts and escalations are reported as necessary to other DTCC support areas.

Production monitoring is conducted with review of automated scheduling software which is used to manage batch processing. Monitoring of the job schedule and/or real-time interfaces is performed by DTCC Technology Operations. Alerts are routed to appropriate personnel for job abends and failures that require resolution. On a daily basis, DTCC Technology Operations verifies that the appropriate resolutions are performed for job abends and failures.

Recovery/restart procedures are in place to allow for recovery of systems to the point of the last processed transaction. Servers with production data are backed up according to a pre-defined schedule and are replicated to at least one other data center (except during a disaster recovery event). Backup failures are researched and resolved in a timely manner.

G. Matrix of Internal Controls Applicable to CTM, TradeSuite ID, ALERT, and Settlement Status Manager Client Services

For ease of reference, the below Exhibit K, Table 2 sets forth the Other Internal Controls implemented for each of the Client Services set forth in Exhibit J, except for the ITP Integration Business Services.

H. Data Integrity

The Applicant also validates the completeness of the information received or disseminated by the Applicant's systems by validating Client messages. Data transferred between DTCC internal systems is governed by the enterprise-wide standard called "File Exchange Verification Standards" that dictates how information received or disseminated is reviewed for accuracy and/or completeness within DTCC systems.

I. Validations

Depending on the specific Client Service and workflow, the Applicant accepts or rejects (as appropriate) transactions based on various validation criteria for each message received:

Regulatory validations, such as OFAC checks, are applied on top of the normal business validations.

J. Instances of Failure of Security Safeguards and Measures

During the last year, there have been no instances in which any security measures or safeguards failed to prevent unauthorized access to the Applicant's systems that perform the Client Services set forth in Exhibit J.