DESIGNATED CONTRACT MARKET
OPERATIONAL CAPABILITY TECHNOLOGY QUESTIONNAIRE

Please provide all relevant documents responsive to the information requests listed within each area below. In addition to the specific documents requested, please provide any other policies, procedures, standards or guidelines, plans, independent assessments (including internal audits), test results, and representations that will assist the Commission in assessing the compliance of your trading platform and related supporting systems with Core Principle 20, SYSTEM SAFEGUARDS. Core Principle 20 requires exchanges to: "(1) establish and maintain a program of risk analysis and oversight to identify and minimize sources of operational risk, through the development of appropriate controls and procedures, and the development of automated systems, that are reliable, secure, and have adequate scalable capacity;[1] (2) establish and maintain emergency procedures, backup facilities, and a plan for disaster recovery that allow for the timely recovery and resumption of operations and the fulfillment of the responsibilities and obligations of the board of trade; and (3) periodically conduct tests to verify that backup resources are sufficient to ensure continued order processing and trade matching, transmission of matched orders to a designated clearing organization for clearing, price reporting, market surveillance, and maintenance of a comprehensive and accurate audit trail."

1. Organizational Structure, System Description, Facility Locations, and Geographic Distribution of Staff and Equipment per the following:

    a. Provide high-level organization charts and staffing level information for all groups that are directly involved in supporting the development, operation and maintenance of the systems, including systems development, quality assurance, system operations, event management, market operations, network and telecommunications, information security, capacity planning, contingency planning (including disaster recovery), market surveillance, and trade practice investigation; include a brief biography with applicable certifications for each key IT staff leader.

    b. Describe or provide a diagram showing the locations of all facilities that house the staff described above and the equipment on which your systems operate. Indicate the nature of the facilities (e.g., headquarters, primary and backup data centers, primary and backup market operations centers, etc.), and a description of your rationale for the distribution of staff and system components across those facilities.

    c. Provide a high-level application flow diagram and the specific information requested below for all systems that perform and support trading, price reporting, regulatory reporting, market surveillance, and trade practice investigation:

        1) System description and overview.

[1] An exchange's program of risk analysis and oversight with respect to its operations and automated systems should address each of the following categories: (1) Information security; (2) Capacity and performance planning; (3) System operations (including configuration management, event management, and incident response); (4) Systems development methodology (including security controls requirements, software change management, and quality assurance) and outsourcing; (5) Business continuity and disaster recovery, including pandemic planning; (6) Enterprise risk management and internal audit; and (7) Physical security and environmental controls.

2) A logical diagram of the software components, including the following information for each component:
    a) Name;
    b) Functional description; and
    c) Upstream and downstream feeds.
3) A representative physical diagram of the hardware components (servers and communications equipment) that exist at both the primary and backup data centers, and for each **representative** hardware component, provide the following information:
    a) Device type (e.g., switch, server, SAN, etc.);
    b) Device O/S;
    c) Functional description;
    d) Internal redundancies (e.g., power supplies, RAID); and
    e) External redundancies (e.g., mirroring, clustering).
4) A physical diagram of the network topology within and between data centers and external entities, and for each connection provide the following information:
    a) Purpose(s) of connection;
    b) Type and bandwidth of each connection; and
    c) Identification of carrier.

2. Risk Analysis and Oversight. Describe your Enterprise Risk Management program as it relates to IT and your entity's approach for assessing and managing the risks associated with technology and cybersecurity, including procedures for risk escalation, adjudication, mitigation, and acceptance; include the following:

    a. Provide a copy of your most recent annual Enterprise Technology Risk Assessment and Enterprise Risk Assessment.

    b. Include a description of Board of Directors and/or Board Committee involvement in oversight of system safeguards and cybersecurity.

    c. Provide a list of Board of Directors and Board Committee members, indicating for each: name, title, and description of any system safeguards and cyber security experience.

    d. Provide copies of all system safeguards-related materials provided to the Board of Directors or applicable Board Committees for the four most recent meetings.

    e. Provide copies of Board of Directors and Board Committee meeting minutes regarding system safeguards from the four most recent meetings.

    f. Describe the process by which the Board is kept apprised of the status of systems safeguards related initiatives and assessments, including any escalation procedures or trigger points that automatically require Board notification and involvement.

    g. Describe any ongoing education or training that Board members receive regarding systems safeguards, including cybersecurity. If a third party consultant is used in matters of system safeguards and cybersecurity risk, include the name, title and applicable qualifications for each consultant.

h. Describe your program of periodic control testing, including:
   1) Selection of controls;
   2) Frequency, scope, and schedule of testing;
   3) Use of any third party assessors; and
   4) Escalation, follow up and resolution of findings.
   5) Provide representative samples of any periodic control testing.

i. Describe your internal audit program, including:
   1) Organizational structure of internal audit;
   2) Audit staff qualifications and use of external staff;
   3) Controls that ensure independence;
   4) Process for development of IT audit plan, including prioritization and allocation of audit resources; and
   5) Follow up and resolution of IT audit findings and recommendations; and quality assurance reviews of the internal audit program and processes.
   6) Provide the results of the most recent quality assurance review.

j. Submit the system evaluation documentation and information requested below for **each of the following systems safeguard categories**: 1) risk management; 2) systems development methodology; 3) information security; 4) system operations; 5) capacity and performance planning; 6) physical security and environmental controls, including data centers; and 7) business continuity and disaster recovery.
   1) Provide your most recent audit or other risk assessment documents for each category, including complete reports (not only executive summaries), management's responses, and mitigation plans and results for addressing findings;
   2) Describe your plans and schedule for ongoing independent audits, other risk assessments, and tests for each category;
   3) Describe how you periodically assess compliance with applicable policies and procedures for each category.

3. System Operations.

a. Configuration Management
   Provide information regarding the controls and procedures that will be used to ensure:
   1) Consistent inventory maintenance;
   2) Adherence to standards for baseline configuration, including hardening;
   3) Pre-installation testing and authorization;
   4) Processes that ensure minimal configuration drift between primary and backup environments; and
   5) Post-installation monitoring and testing

b. System software change management
   Provide information regarding the controls and procedures that will be used to ensure the reliability of system software, including:
   1) Testing;
   2) Independent review for quality assurance;
   3) Approval for production installation;

4) Processes that ensure minimal configuration drift between primary and backup environments;
5) Post-change monitoring, including testing to confirm planned vs. actual system configuration;
6) Separation of duties;
7) Controls in place to ensure quality, consistency, and security of code developed by third party developers; and
8) Controlled access to code libraries.

c. Patch management program
Provide information regarding the controls and procedures that will be used to ensure the timely application of essential patches, including:
1) Staffing;
2) Awareness;
3) Analysis of required patching to operational systems and any impact to computing environments;
4) Testing and Approval;
5) Emergency patch processes and procedures, including notification, analysis, testing, approval, and implementation;
6) Implementation and fallback procedures; and
7) Communication and reporting.

d. Event and problem management
Provide information regarding the controls and procedures that will be used to ensure the timely notification about operational events and resolution of operational problems, including:
1) Staffing;
2) Roles and responsibilities;
3) Use of monitoring systems;
4) Tracking and escalation;
5) Resolution; and
6) Internal and external reporting, including notification of appropriate regulators.

e. Provide information about your security incident response program, including:
1) Staffing;
2) Roles and responsibilities;
3) Training;
4) Procedures (including detection, analysis, containment, and recovery);
5) Communication/notification and reporting, including notification of appropriate regulators, law enforcement, and appropriate information sharing organizations; and
6) Testing of security incident response procedures.

f. Describe your cybersecurity threat intelligence capabilities, including:
1) Staffing (in-house and outsourced services);
2) Roles and responsibilities;
3) Training;
4) Intelligence gathering and analysis methodology;

5) Dissemination of intelligence within the organization and with appropriate information sharing organizations, and
6) Evaluating intelligence for tactical and strategic action.

g. Describe your participation in any information sharing organizations, e.g., FS-ISAC.

4. Systems Development Methodology

a. Describe your process, including roles and responsibilities, for identifying and approving functional, security, and capacity/performance requirements.

b. Describe your software change management process, including quality assurance and issue tracking and resolution.
1) Provide information regarding the testing methodology, including management controls, used to verify the system's ability to perform as intended (regarding functionality, security, and capacity and performance requirements).
2) Provide copies of current representative samples of your test results documentation.
3) Identify what group is responsible for recording, correcting, and retesting errors, and detail their procedures for those activities.

c. Describe the documentation required during the development of new software and as part of the software release package for installation, operation, and maintenance.

d. Describe the controls in place for promotion of application software into the production environment, including approval, access controls, and post-implementation monitoring.

e. Outsourcing and Vendor Management
1) Provide a copy of each service agreement currently in place for any IT services provided by a third party.
2) Describe your process for pre-contract due diligence and screening of IT service providers.
3) Describe your process for monitoring the performance of service agreements, including roles and responsibilities, scope and frequency of review, and remediation of identified deficiencies.
4) Describe inclusion of vendor relationships and outsourced systems in your ongoing risk management process.
5) Describe any information systems security testing and ongoing monitoring you may require and/or conduct of vendors.
6) Provide a list of all vendors who have any sort of connection or access to your systems and describe how you manage and mitigate the risks to your systems posed by this access on an ongoing basis.

5. Information Security

a. Provide documentation (policies, standards, guidelines) that attests to the development of and adherence to an ongoing information security program.

b. Provide a logical security architecture diagram and description.

c. Describe your background investigation program's controls and procedures to include credit checking for the following:
    1) Pre-assignment of personnel to sensitive roles; and
    2) Recurring periodic investigations for staff in sensitive roles.

d. Provide information regarding security awareness training and education:
    1) Describe the security awareness training provided to system users, including periodic refresher training.
    2) Identify the roles of personnel that have significant system security or system development responsibilities and describe the security training they are required to complete.

e. Provide information regarding the access controls and procedures that are used to ensure the identification, authorization, and authentication of system users and any third party service providers.

f. Provide information regarding the procedures that are used to ensure proper account management, including:
    1) Establishing, changing, reviewing and removing accounts (including emergency and other temporary accounts);
    2) Password complexity and life cycle standards; and
    3) Maintaining user awareness of the authorized uses of the system.

g. Provide information regarding the administrative procedures (such as adherence to least privilege and separation of duties concepts) and automated systems that will be employed to prevent and detect the unauthorized use of the system.

h. Provide information (including specific products used, guidelines for use, and roles and responsibilities) regarding the use and management of safeguards and security tools used to protect the critical data and system components, including:
    1) Encryption and data compression (data at-rest and in-transit);
    2) Denial of service protection;
    3) Firewalls;
    4) Routers;
    5) DMZs and network segmentation;
    6) Intrusion detection;
    7) Event logging and log analysis, including:
        a) Scope of log coverage (e.g., production/development; servers/firewalls);
        b) Focus of event details captured (e.g., unauthorized activities, system issues);
        c) Monitoring of system logging alerts (e.g., log failure alert); and
        d) Frequency and level of log review, analysis, and reporting.
    8) Virus protection;
    9) Encryption and control of portable mobile devices;
    10) Encryption and control of portable external media (e.g., USB drives, optical media, external hard drives, etc.);
    11) Data Loss Prevention (DLP) tools; and

12) Ongoing testing of the efficacy of safeguards and security tools for the areas enumerated above.

i. Provide policies, guidelines, and procedures for authorization and use of remote access capabilities to manage the system, including hardware and software tools that protect the information and system while using those capabilities. In your response, also address policies, guidelines or procedures governing third party access to your systems.

j. Provide information about your procedures for sanitization, destruction, and disposal of equipment and media.

k. Provide information regarding your use of internal and third party vulnerability scanning and testing to identify and eliminate vulnerabilities in the configuration of your computing and communications equipment. Address each of the following:
   1) Scope of testing;
   2) Frequency of use;
   3) Methodology and tools;
   4) Distribution of reports;
   5) Remediation of findings by severity or risk posed; and
   6) Tracking of mitigation activities, including notification of senior management or the Board.

l. Provide information regarding your use of internal and third party external and internal penetration testing to identify and eliminate vulnerabilities in the architecture and configuration of your computing and communications equipment. Address each of the following:
   1) Scope of testing;
   2) Frequency of use;
   3) Methodology and tools;
   4) Distribution of reports;
   5) Remediation of findings by severity or risk posed; and
   6) Tracking of mitigation activities, including notification of senior management or the Board.

m. Provide the results of the two most recent internal or third party vulnerability scans (for our assessment of progress made), including complete reports (not only summaries), management's responses, and mitigation plans and results for addressing findings.

n. Provide the results of the two most recent internal or third party penetration tests (for our assessment of progress made), including complete reports (not only summaries), management's responses, and mitigation plans and results for addressing findings.

o. Provide information about any internal password scanning you perform, including:
   1) Frequency of use;
   2) Tools used;
   3) Scope; and
   4) Follow-up.

p. Provide information regarding the manual and automated processes that will ensure:
   1) Fair and equitable trading;
   2) Your ability to detect and investigate persons suspected of violating trading rules; and
   3) That information necessary to conduct trade practice investigations (i.e., audit trail information) is captured and securely stored for five years.
      a. Identify the specific audit trail information captured.
      b. Describe the controls that provide for reliable collection of audit information, including those that ensure sufficient capacity and alerting of audit failures.
      c. For each copy of the audit trail information, describe the processes that protect the information from accidental and deliberate alteration or destruction prior to its planned disposal. Include information about:
         i. Access controls (physical and logical);
         ii. Environmental controls (e.g., fire protection) provided at storage locations;
         iii. Schedule and procedures for secure movement of information;
         iv. Retention period; and
         v. Distance between storage locations.

6. Physical Security and Environmental Controls

   a. Provide information regarding the physical security controls used in the communications and central computer facilities to protect system components and critical infrastructure. In your response, please address:
      1) Perimeter and external building controls and monitoring, including:
         a) Lights;
         b) Cameras;
         c) Motion detectors;
         d) Guards;
         e) Fences, gates, and other barriers; and
         f) Building entrances, including loading docks.
      2) Internal building controls and monitoring, including:
         a) Engineering and physical security staffing, including shift coverage, minimum qualifications and training;
         b) Metal detectors;
         c) Door locks;
         d) Visitor controls, including scheduling, identification, logbooks, and escort requirements;
         e) Compartmentalization of computing, communications, and building infrastructure equipment;
         f) Cameras, video recording, and monitoring stations;
         g) Access authorization and review procedures; and
         h) Mail and package handling procedures.

b. Provide copies of any internal or third party physical security assessments conducted for each of your operating locations.

c. Describe plans for third party physical security assessments for each of your operating locations.

d. Provide information regarding the environmental controls used in the communications and central computer facilities to ensure reliable availability of system components and critical infrastructure. Address redundancy, monitoring, maintenance, and testing of:
   1) Electrical supply, including:
      a) Sources and paths of commercial power;
      b) Generators (and associated on-site fuel supply and fuel delivery contracts);
      c) Power distribution units;
      d) Uninterruptible Power Supply units; and
      e) Emergency shutoff controls.
   2) Cooling equipment, including:
      a) HVAC units;
      b) Air handlers;
      c) Chillers; and
      d) Other associated items such as water supply and humidifiers.
   3) Fire control equipment, including:
      a) Smoke and heat detection;
      b) Fire suppression; and
      c) Water damage protection.

e. Provide copies of any recent third party assessments of your communications and central computer facilities, including results and plans for remediation of any findings made.

f. Provide information regarding any Single Point of Failure reviews or assessments made of your communications and central computer facility infrastructure.

7. Capacity Planning and Testing

a. Provide the capacity levels and associated performance (i.e., response time) for each of the following system activities, including target, average daily, historical high, and system stress-tested sustained and peak levels:
   1) Simultaneous workstation sessions;
   2) Market participant transactions;
   3) Trade matches;
   4) Quote vendor transactions; and
   5) Data mirroring transactions.

b. Describe any formal process you employ for the ongoing review of capacity and performance levels.

c. Describe current system bottlenecks, and the methods in which they are monitored.

d. Describe at what levels the addition of new system resources would be triggered to ensure adequate capacity and performance.

e. Describe the methods by which additional capacity and performance resources could be activated in an emergency situation and state how long those processes would take.

8. Business Continuity and Disaster Recovery ("BC-DR"). Provide the following information:

a. A description of your DR sites, including the following information for each site:
   1) State of readiness (hot, warm, cold);
   2) Whether a commercial or self-managed site; and
   3) Distance from production site.

b. A description of the public infrastructure (e.g., water, electric) supporting each of your BC-DR sites, including redundancy, resilience, and physical security.

c. A list of the mission-critical systems that each BC-DR site will support on a routine, non-disaster basis, and a description of your reasons for this overall data center strategy.

d. A list of the mission-critical systems that each of your BC-DR sites will support in the event of a disaster.

e. Copies of all agreements, including service level agreements, with third parties to provide services in support of your BC-DR plans.

f. A description of your strategy for ensuring the availability of essential software and data, including security and testing of backups.

g. A description or assessment of the maximum potential data loss in the event of a disaster, including data loss of in-transit data

h. A description of your strategy for staffing DR sites in the event of a disaster, including a pandemic.

i. A description of any plans or capabilities for remote management and operation of your primary or DR sites in the event that they become inaccessible but remain functional. Include information regarding the systems security controls that will be applied to internal and third party (including service provider) users.

j. Briefing materials for senior management regarding BC-DR and pandemic plans.

k. BC-DR and pandemic training materials prepared for employees.

l. A description of your procedures for ensuring the currency and availability to team members of essential documentation.

m. Your technology-related BC-DR plans, including roles and responsibilities, staffing assignments, recovery procedures, test plans, external dependencies and any pandemic plans.

n. Your Emergency Communications Plan, including emergency contact information.

o. A description of external communications and reporting regarding BC-DR events, including notification of customers and appropriate regulators.

p. A description of how your BC-DR plan is coordinated with members' BC-DR plans.

q. A description of your strategy for testing your DR sites, including frequency, types of tests, and scope of staff and market participant involvement.

r. A copy of the most recent SSAE16 Type II reports for each of your data centers, including, if applicable, any actions taken to remediate findings in the report.

s. Documentation from the three most recent operational tests conducted with respect to your DR sites, including the test plan, the results report, and the mitigation plan and results.

t. Documentation from your participation in the most recent industry wide test relating to BC-DR matters, including the test plan, the results report, and the mitigation plan and results.

u. A description of any instances of activation of your BC-DR plans, including the results report and the mitigation plan and results.

w. What is your recovery time objective ("RTO") for each of the following:
    1) Resumption of trading.
    2) Completed clearing of transactions executed prior to disruption.
    3) Resumption of clearing of new transactions.
    4) Resumption of market surveillance.
    5) Access to audit trail information and resumption of trade practice surveillance.