Exhibit V

Technology Questionnaire

Please provide all relevant documents responsive to the information requests listed 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 Division in assessing your organization's compliance with the system safeguards requirements of the Commodity Exchange Act and the applicable Core Principles and CFTC regulations.

Organization and systems overview

This section requests documents relating to your corporate structure and governance model as it relates to your system safeguards program of risk analysis and oversight. In some cases, supervision of the registered entity's system safeguards program may be provided by governance bodies external to the registered entity (for example, by the Board of Directors of a parent company). In addition, in some cases services that are part of the registered entity's system safeguards program may be provided to the registered entity by another entity in the corporate structure. A clear description of the entire corporate structure involved in any aspect of the system safeguards program will assist the Division in both conducting the oversight required and limiting the scope of that oversight to the parts of the corporate structure that play a role with respect to the registered entity's technology risks.

✔	ID	Item
	ORG.01	A high-level organizational chart showing all parts of the corporate organizational structure involved with any aspect of the registered entity's program of system safeguards risk analysis and oversight, their corporate relationships, their geographic location (city/state/country), and their role with respect to the registered entity's system safeguards program.
	ORG.02	A list of all Boards, Board-level committees, other governance bodies, and senior management positions responsible for any aspect of oversight of the registered entity's program of system safeguards risk analysis and oversight, and the members or staff occupying each such board, committee, or management position.
	ORG.03	A high-level staffing chart showing all groups involved in development, operation, or maintenance of the registered entity's automated systems, and the number of staff in each group.
	ORG.04	A description of relevant skills, experience, and certifications held for the leaders of each group identified in the chart for item ORG.3.
	ORG.05	A list or diagram of all facilities housing the staff in item ORG.3 or housing any equipment used by the registered entity's automated systems, indicating the location and nature of each facility (e.g., headquarters, primary data center, backup data center, etc.).
	ORG.06	A brief description of the rationale for the distribution of staff and automated system components across the facilities included in item ORG.5.

	ORG.07	A high-level description of information flows and shared resources across business units included in the chart for item ORG.1.
	ORG.08	A list of technology services provided by affiliates to the registered entity.
	ORG.09	A list of technology services provided by the registered entity to affiliates.

Enterprise risk management and governance

In addition to the documents specified below, please provide any other policies, procedures, standards or guidelines, plans, independent assessments (including internal audits), test results, and representations that will assist the Division in assessing the registered entity’s compliance with system safeguards requirements relating to enterprise risk management and governance.

✔	ID	Item
	ERM.01	Risk management strategy and objectives.
	ERM.02	Risk appetite/tolerance statement.
	ERM.03	Risk assessment methodology.
	ERM.04	Enterprise Technology Risk Assessment ("ETRA").
	ERM.05	Processes and procedures for ETRA analysis, documentation, governance, review, updating, and approval.
	ERM.06	Risk treatment or mitigation plan(s).
	ERM.07	Risk acceptance memos and risk acceptance-related management reports.
	ERM.08	Risk escalation process, senior management notification process, and Board notification process.
	ERM.09	IT/risk committee charter(s).
	ERM.10	A description of the system safeguards experience and system safeguards-related expertise of each Board member.
	ERM.11	Complete agendas and minutes for all Board, IT or Risk Committee, and Audit Committee meetings since the last update of this request.
	ERM.12	All prepared materials provided or presented to the Board, the IT or Risk Committee, or the Audit Committee relating to system safeguards.
	ERM.13	Internal audit plan, policies and procedures.
	ERM.14	Schedule of IT- or system safeguards-related internal audits.
	ERM.15	List of IT- or system safeguards-related assessments performed by third parties.

	ERM.16	IT- or system safeguards-related internal audit or third-party assessment reports.
	ERM.17	List of IT- or system safeguards-related internal audit or third-party assessment findings and recommendations.
	ERM.18	Management review and corrective action reports for all internal audit or third-party assessment findings and recommendations.
	ERM.19	IT/risk awareness and training materials for all levels of the corporate structure.
	ERM.20	Vendor risk management policy and procedures.
	ERM.21	Questionnaires and other assessment templates used to assess vendor fitness.
	ERM.22	List of all technology service providers ("TSPs").
	ERM.23	Acquisition contracts and service-level agreements with critical TSPs.
	ERM.24	Internal risk assessment reports for critical TSPs.
	ERM.25	Third-party assessment reports (e.g., SSAE16/SOC2) for critical TSPs.
	ERM.26	List of all vendors with access to registered entity systems.

Information security

In addition to the documents requested below, please provide any other policies, procedures, standards or guidelines, plans, independent assessments (including internal audits), test results, and representations that will assist the Division in assessing the registered entity’s compliance with system safeguards requirements relating to information security.

✔	ID	Item
	ISC.01	Information security program policies and procedures.
	ISC.02	Data classification and systems categorization policies.
	ISC.03	Access control policy.
	ISC.04	Account management policy and procedure.
	ISC.05	Password policies, for both user and service accounts.
	ISC.06	Privileged access management policy.
	ISC.07	Multi-factor authentication standard and tools.
	ISC.08	Endpoint protection policy and related tools and techniques.

	ISC.09	Application security policy.
	ISC.10	Network security policy.
	ISC.11	Data loss prevention (DLP) strategy and tools.
	ISC.12	Boundary defense strategy and tools.
	ISC.13	Wireless (WLAN) and mobile access policy.
	ISC.14	Remote access policy.
	ISC.15	Employee screening and security clearance policies and procedures.
	ISC.16	Description of employee joiner/mover/leaver workflows.
	ISC.17	Acceptable use and privacy policy (internal).
	ISC.18	Data encryption policy.
	ISC.19	Data destruction policy.
	ISC.20	Equipment and media disposal policy.
	ISC.21	Media protection policy.
	ISC.22	Mobile device security policy.
	ISC.23	Information security training policies and procedures.
	ISC.24	Information security awareness and training materials.
	ISC.25	Vulnerability detection and patch management standard(s).
	ISC.26	Vulnerability scanning policy and procedure.
	ISC.27	Vulnerability scan results and management reports.
	ISC.28	Patch management policy and procedure.
	ISC.29	Patch validation results and management reports.
	ISC.30	Penetration testing policy and procedure.
	ISC.31	Penetration test results and management reports.
	ISC.32	Brief description of process for identifying key controls.
	ISC.33	Controls testing plan, including a description of planned testing of key controls.

	ISC.34	Controls testing results and management reports.
	ISC.35	Security Incident Response Plan.
	ISC.36	Security Incident Response Plan exercise or testing results and management reports.
	ISC.37	Description of threat intelligence program or related activities.

Business continuity and disaster recovery

In addition to the documents requested below, please provide any other policies, procedures, standards or guidelines, plans, independent assessments (including internal audits), test results, and representations that will assist the Division in assessing the registered entity’s compliance with system safeguards requirements relating to business continuity and disaster recovery.

✔	ID	Item
	BCM.01	Description of overall strategy for ensuring the continued delivery of critical services in the event of a disruption, including recovery point and recovery time objective(s).
	BCM.02	Description of management oversight for BC-DR planning.
	BCM.03	Description of alternate work sites and remote access capabilities.
	BCM.04	Business continuity and disaster recovery plan(s).
	BCM.05	Business impact analyses (or any scenario-based analyses of service impact), including any identified external dependencies.
	BCM.06	Single point of failure reviews, or other assessments of component-level availability.
	BCM.07	List of all vendors expected to provide services in support of BC-DR plan(s).
	BCM.08	List of telecommunications, power, water, and other essential infrastructure services and service providers that support BC-DR plan(s).
	BCM.09	Description of how the registered entity ensures that its business continuity and disaster recovery plan takes into account the recovery plans of its telecommunications, power, water, and other essential service providers.
	BCM.10	Data recovery and synchronization procedure(s).
	BCM.11	Description of overall approach to BC-DR exercises, including scenario development, frequency, and schedule.
	BCM.12	BC-DR exercise results and senior management reports.
	BCM.13	BC-DR employee resources and training materials.
	BCM.14	Internal and external notification standards.

	BCM.15	Description of alternative communication methods.
	BCM.16	Description of (a) how the registered entity coordinates its business continuity and disaster recovery plan and plan testing with members or market participants on whom it depends to provide liquidity (if it is a DCM or SEF), or with entities or parties that report swap data to it (if it is an SDR).
	BCM.17	Description of participation in business continuity or disaster recovery testing involving other financial sector firms.

Capacity and performance planning

In addition to the documents requested below, please provide any other policies, procedures, standards or guidelines, plans, independent assessments (including internal audits), test results, and representations that will assist the Division in assessing the registered entity’s compliance with system safeguards requirements relating to capacity and performance planning.

✔	ID	Item
	CPP.01	Capacity planning policy and procedures.
	CPP.02	List of capacity and performance metrics tracked on an ongoing basis.
	CPP.03	Description of tools and techniques used to establish capacity baselines.
	CPP.04	Description of tools and techniques used to forecast future resource demands.
	CPP.05	Description of any known bottlenecks and/or priorities for future upgrades.

Systems operations

In addition to the documents requested below, please provide any other policies, procedures, standards or guidelines, plans, independent assessments (including internal audits), test results, and representations that will assist the Division in assessing the registered entity’s compliance with system safeguards requirements relating to systems operations.

✔	ID	Item
	OPS.01	Description of overall approach to IT systems/service management.
	OPS.02	Description of tools and techniques used to monitor the stability and health of services.
	OPS.03	Description of tools and techniques used to maintain a comprehensive and up-to-date IT asset inventory.
	OPS.04	Description of tools and techniques used to fulfill internal and external service requests.

	OPS.05	IT service catalog, or list of critical resources and services.
	OPS.06	Platform architecture diagram(s).
	OPS.07	Network topology diagram(s).
	OPS.08	IT inventory / asset management policy and procedure.
	OPS.09	Network monitoring policy and procedures.
	OPS.10	Log retention and monitoring policy.
	OPS.11	Configuration management policy.
	OPS.12	Change control policy.
	OPS.13	Change control oversight or change approval board (CAB) meeting agendas.
	OPS.14	Release and deployment policy and procedure.
	OPS.15	Event and problem management policy and procedure.

Systems development and quality assurance

In addition to the documents requested below, please provide any other policies, procedures, standards or guidelines, plans, independent assessments (including internal audits), test results, and representations that will assist the Division in assessing the registered entity's compliance with system safeguards requirements relating to systems development and quality assurance.

✔	ID	Item
	SDM.01	Description of overall approach to systems development, including the extent of ongoing, continuous development activity affecting critical services.
	SDM.02	Description of software development lifecycle, including the use of any alternative methodologies (e.g., spiral, iterative, agile).
	SDM.03	Software development lifecycle standard, and any related policies and procedures.
	SDM.04	Project management standard, and any related policies and procedures.
	SDM.05	Description of tools and techniques used to schedule and monitor project tasks.
	SDM.06	Documentation standard, and any related policies and procedures.
	SDM.07	Systems design standard, and any related policies and procedures.
	SDM.08	Quality assurance standard, and any related policies and procedures.

	SDM.09	Testing standard, and any related policies and procedures.
	SDM.10	Description of overall approach to quality assurance and testing, including the extent of end-user participation and the use of automation.
	SDM.11	Software and services acquisition policy.
	SDM.12	Documentation production and maintenance procedure, or description of process.

Physical security and environmental controls

In addition to the documents requested below, please provide any other policies, procedures, standards or guidelines, plans, independent assessments (including internal audits), test results, and representations that will assist the Division in assessing the registered entity’s compliance with system safeguards requirements relating to physical security and environmental controls.

✔	ID	Item
	PHY.01	Description of overall approach to facilities management, including standards for site selection, construction, and long-term operability (addressing issues of co-location, proximity, etc.), building maintenance and engineering, routine inspection and monitoring, and other due diligence measures.
	PHY.02	Description of overall approach to physical security, including the key preventive, detective, and corrective security measures at each facility housing personnel, equipment, records, and data in support of IT operations.
	PHY.03	Description of overall approach to addressing risks from environmental threats (e.g., fire, flood, and uncontrolled temperature), including detection mechanisms, suppression techniques, and real-time monitoring and alerting capabilities.
	PHY.04	Description of overall approach to maintaining stable environmental conditions, including preventive and detective measures to reduce interference from dust, vibration, noise, and electromagnetic radiation.
	PHY.05	Description of engineering and physical security staffing, including shift coverage, qualifications, and training.
	PHY.06	Physical and environmental protection policy.
	PHY.07	Employee access control policy.
	PHY.08	Visitor access control policy.
	PHY.09	Access logging and monitoring procedures, or description of process.
	PHY.10	Mail and package handling policy and procedure (inbound and outbound).