Form CA-1 – Exhibit K

Cboe Description of Systems and Datacenters

CCUS's information technology infrastructure currently consists of SCI Critical Systems, both direct and indirect, with multiple deployable components. These systems will be hosted in a virtual private cloud ("VPC") environment across a minimum of (2) geographically disparate regions. The system will have the ability to run with either region as the "primary" and failover either parts or all of the application to the "secondary" region when needed. Data will be replicated to the secondary region and backed up to meet the recovery objectives. CCUS relies on Cboe's supporting technology infrastructure in physical data centers and facilities to provide access into CCUS's technology infrastructure. These systems are also provisioned with geographically diverse data centers sites.

Information Security

Cboe's policies, procedures, and controls are built upon industry best practices and are intended to prevent unauthorized access to its information and networks across both physical datacenters and the VPC environment. Cboe will convey comparable expectations to its vendors through outsourcing agreements and associated service level agreements, while also maintaining oversight and monitoring of vendor activities.

The VPC environment provider maintains policies, procedures, and controls aligned with best practices that support Cboe's control objectives. In addition, one of Cboe's vendors will deliver information security services designed to meet Cboe's requirements for protecting the confidentiality, integrity, and availability of information. These services are delivered through a structured program aimed at mitigating security risks and threats. The vendor's approach incorporates multiple, complementary layers of security controls across people, technology, and operations. Vendor-provided services are designed to prevent unauthorized access and include but are not limited to: identity and access management ("IAM"), security monitoring, and security architecture.

Physical Security

Cboe's policies, procedures, and controls also encompass physical security measures designed to prevent unauthorized access to its information and networks in both its physical datacenters and the VPC environment. Cboe will review vendor policies and procedures to ensure the physical security of vendor operations performed for or on its behalf meet its requirements. These measures are intended to safeguard personnel, resources, infrastructure, brand, reputation, and business

operations from individuals, groups, or events that could disrupt operations or result in damage and/or financial loss, including through unauthorized access.

These controls are further designed to identify and mitigate risks before they develop into credible threats by assessing vulnerabilities, evaluating potential impacts, and distributing timely information to employees, leadership, and business partners. Cboe will also oversee its VPC provider to ensure compliance with its physical security policies, procedures, and controls.

In general, and consistent with best practices, physical security for both Cboe's datacenters and the VPC environment is implemented through a combination of related controls. Datacenters are located in nondescript facilities. Physical access is tightly controlled at both the perimeter and building entry points by professional security personnel utilizing video surveillance, intrusion detection systems, and other electronic monitoring tools. All visitors and contractors must present identification, and all access to datacenters is recorded and subject to routine audit. Access to datacenter facilities and related information is granted only to employees and contractors with a legitimate business need. When that need no longer exists, access is promptly revoked, even if the individual remains employed by the vendor.