CME Securities Clearing CA-1 – EXHIBIT K

Exhibit Request:

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.

Response:

CMESC Description of Systems and Datacenters

The CMESC information technology infrastructure is currently made up of SCI Critical Systems with multiple deployable components. CMESC systems will be hosted in a virtual private cloud ("VPC") environment and in physical datacenters. One instance of each of the physically hosted systems will be deployed to a primary data center. Backups for the physically hosted systems will be available in another, geographically disparate datacenter. VPC environment backup systems will also be in geographically disparate locations. Another geographically disparate location will house disaster recovery ("DR") infrastructure and servers hosting backup data from both the VPC environment and the physical datacenter servers.

Information Security

Built on best practices, CMESC policies, procedures and controls are designed to prevent unauthorized access to its information and networks at its physical datacenters and within the VPC environment. CMESC will communicate similar expectations to its vendors, including through outsourcing agreements and related service level agreements, and will oversee and monitor vendors.

The VPC environment provider has policies, procedures and controls in place in line with best practices that will enable it to meet the control objectives of CMESC. Similarly, one of CMESC's vendors will provide information security services to CMESC that meet CMESC's control objectives to safeguard the confidentiality, integrity and availability of information through a structured program designed to mitigate security risks and threats. The vendor will provide in depth information security through multiple and complementary layers of security controls focusing on people, technology, and operations. CMESC's vendors will provide services designed to prevent unauthorized access, including (a) identity and access management ("IAM"), (b) security operations and (c) security architecture.

Physical Security

CMESC's policies, procedures and controls include physical security components designed to prevent unauthorized access to its information and networks both at its physical datacenters and within the VPC environment. CMESC will conduct vendor oversight to monitor physical security over vendors operations for or on behalf of CMESC that are designed to protect personnel, resources, infrastructure, brand, reputation, and business operations from any persons, groups, or events that may disrupt its business operations or cause damage and/or economic loss, including by unauthorized access. The controls are also designed to prevent and deter risks before they manifest into credible threats against our organization by identifying threats, assessing vulnerabilities, determining potential impacts, and disseminating timely information to employees, leaders, and business partners. CMESC will also oversee and manage its VPC provider to monitor compliance with CMESC policies, procedures, and controls related to physical security.

Generally, in line with best practices, physical security of both CMESC's physical datacenters and the VPC environments will be provided through several related controls. Datacenters are housed in nondescript buildings. Physical access to them is strictly controlled both at the perimeter and at building ingress points

by professional security staff who use video surveillance, intrusion detection systems, and other electronic means. All visitors and contractors are required to present identification, and all physical access to data centers is logged and routinely audited. Data center access and information is provided only to employees and contractors who have a legitimate business need for these privileges. When an employee no longer has a business need, his or her access is immediately revoked, even if he or she continues to be an employee of the vendor.