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.

1. ICE's Corporate Information Security Policy (the "CISP"), which is applicable to ICC (and therefore both the CDS Business and the Treasury Business), covers the information security policies for the creation, transfer and storage of sensitive data applicable to all users. The CISP provides ICE employees with a standardized, accountable, documented and secure guidelines for conducting business. The CISP covers all information components of ICE, including all information environments operated by ICE or contracted with a third party by ICE. The term "information environment" defines the total environment and includes, but is not limited to, all documentation, physical and logical controls, personnel, hardware (*e.g.*, desktop, laptop, company-owned PDA, network devices), and software. Information security officers are responsible for the implementation, maintenance and enforcement of the CISP. The CISP covers, among other things, the following areas:

    a. Security Awareness Policy – this covers policies on data classification, handling, retention and access safeguards (*e.g.*, web-based content filtering, malicious software protection mechanisms and user endpoint protection software and ICE physical equipment policies). Pursuant to this policy, employees are required to complete annual training and testing.

    b. Access Control Policy – this covers policies on access to data available through ICE's systems, including unauthorized access, unauthorized changes and disclosure. Because ICE operates various systems on behalf of its regulated subsidiaries and, in certain circumstances, third parties, access to data available through such systems must be appropriately limited to maintain the confidentiality of the same on behalf of ICE and the business in question, and to ensure that any data accessed by ICE personnel, whose ICE accounts are set up on a need-to-know basis with limited privileges, is used in accordance with all applicable law and ICE's contractual and regulatory obligations.

    c. Remote Access Policy – because remote access is made available to employees on a business need basis at the discretion of the employee's manager, ICE has a formal access request and ticketing system along with policies and requirements around how remote access is controlled and how confidential ICE resources may be accessed remotely (including from non-ICE networks).

    d. Data Protection Policy – this policy focuses on the enhancement of confidentiality, integrity and availability of data and the minimization of risks to information in an efficient manner and provides for the responsibilities of personnel in connection with the requirements and procedures on data classification, authentication, control, monitoring, protection, retention and destruction. The policy also focuses on statutory and business-imposed minimum retention periods for certain categories of documentation; statutory and business-imposed obligations to secure personal data and avoid retaining it for longer

than necessary; regulatory and business-imposed obligations to retain records relating to disciplinary matters and anti-money laundering controls; all data stored in paper or electronic format can be enforcedly disclosed in the course of legal, criminal or regulatory investigations; and the implications of destroying documents in contravention of the CISP.

e. Network Security Policy and Systems Security Policy – these policies cover how network devices and computing systems are configured and establish certain standards and controls for the minimum configuration and security features, mechanisms and assurances that must be employed on systems which process, store or communicate ICE information to minimize unauthorized access to ICE proprietary information and technology. All internal services at ICE are owed by an operational group that is responsible for system administration and establishing and maintaining any other operational and configuration guidelines based on the business needs.

f. Security Testing Policy – ICE maintains a comprehensive testing program to validate the effectiveness of its controls on a regular and frequent basis to identify risks and vulnerabilities that could allow a malicious actor to interfere with operations or fulfillment of regulatory or legal obligations, impair or degrade reliability, capacity, or security of key systems, exfiltrate or compromise the integrity of data, or undertake any other unauthorized action. The ICE program combines automated testing with targeted, intelligence-led attack simulation. The Risk Assessment program includes a reporting component to ensure governance is made aware of acutely severe findings or thematic remediation delinquency. Elements of the testing program include vulnerability assessments and penetration testing.

2. There have been no incidents in the past year of unauthorized access to the systems.