Regulation SCI
HANDBOOK

December 2, 2015

*This presentation is for internal use only.

What is Regulation Systems Compliance & Integrity (SCI?)

- A regulation under the U.S. Securities Exchange Act of 1934 (Exchange Act).
- Advances the goals of the national market system by enhancing the capacity, integrity, resiliency, availability, and security of the automated systems of entities important to the functioning of the U.S. securities markets.
- Reinforces the requirement that such automated systems operate in compliance with the Exchange Act and related rules and regulations, as well as ISE rules, as applicable.
- Strengthens the infrastructure of the U.S. securities markets and improves its resilience when technological issues arise.
- Effective Date: February 3, 2015.
- Compliance Date: November 3, 2015.

Key Regulation SCI Definitions – SCI System, Indirect SCI System

SCI Systems mean all computer, network, electronic, technical, automated, or similar systems at ISE (or operated by or on behalf of ISE*) that **directly support:**

1. Trading
2. Order Routing
3. Market Data
4. Market Regulation
5. Market Surveillance

(Also included in the definition is clearance and settlement which is not applicable to ISE because ISE is not a clearing agency).

**For example*: Exegy (trading) and FINRA (market surveillance).

See Regulation SCI Systems List in J:\Regulation SCI

Indirect SCI Systems mean any ISE systems (or systems operated on or behalf of ISE) that, if breached, would be reasonably likely to pose a security threat to SCI systems.

- See *Regulation SCI Compliance Manual* for details on ISE's indirect SCI systems.

Key Regulation SCI Definitions – SCI Event, Responsible SCI Personnel

SCI Event: An event at ISE that constitutes**:**

1. A **systems disruption**
   a. An event in ISE's SCI systems that *disrupts,* or *significantly degrades*, the *normal operation* of an SCI system.
2. A **systems compliance issue**
   a. An event at ISE that has *caused* any ISE SCI system to *operate* in a manner that *does not comply* with the *Securities Exchange Act of 1934* and the *rules and regulations thereunder* or *ISE's rules* or *governing documents*, as applicable.
3. A **systems intrusion**
   a. Any unauthorized entry into ISE's SCI systems or indirect SCI systems.

Responsible SCI Personnel: ISE senior managers, and their designees, who have responsibility for a particular SCI system or indirect SCI system.

- See *Regulation SCI Compliance Manual* for list of ISE responsible SCI personnel.

ISE Obligations under Regulation SCI

Regulation SCI requires ISE to, among other things:

- establish, maintain, and enforce certain minimum written policies and procedures;
- take corrective action when an SCI event occurs;
- notify the SEC and ISE members about an SCI event;
- periodically notify the SEC about material changes to SCI systems;
- maintain geographically diverse backup and disaster recovery sites;
- conduct periodic SCI reviews of ISE's compliance with Regulation SCI;
- maintain records of all documents relating to compliance with Regulation SCI (in accordance with ISE's document retention policy).

Capacity, Integrity, Resiliency, Availability, & Security ("CIRAS") of ISE SCI Systems and Indirect SCI Systems

To ensure that its SCI systems and indirect SCI systems have levels of CIRAS adequate to maintain operational capability and promote the maintenance of fair and orderly markets, ISE must establish, maintain, and enforce **written** policies and procedures that include, at a minimum:

1. Reasonable current and future technological infrastructure **capacity planning**.
2. Periodic **capacity stress tests** to ensure timely, accurate and efficient transaction processing.
3. A program to review and keep current **systems development and testing methodology.**
4. **Regular review and testing** (incl. backup systems) to identify vulnerabilities posed by internal/external threats, physical hazards, and natural or manmade disasters.
5. **Business continuity and disaster recovery plans** that achieve next day resumption of trading or 2-hour resumption of critical SCI systems following a wide-scale disruption.
6. Standards that result in designing, developing, testing, maintaining, operating and surveilling such systems to facilitate successful, collection, processing, and dissemination of **market data.**
7. **Monitoring** of such systems to identify *potential* SCI events.

CIRAS: Current and Future Technological Infrastructure Capacity Planning

- Helps ISE determine whether its SCI systems and indirect SCI systems have the ability to process transactions in an accurate, timely, and efficient manner.
- Ensures market integrity.
- Does not apply to *non*-technological infrastructure at ISE.

Current related ISE policies and procedures:

1. ISE Capacity Planning Policy
2. ISE Information Security Policy

CIRAS: Periodic Capacity Stress Tests

- Helps ISE determine whether its SCI systems and indirect SCI systems are able to process transactions in an accurate, timely, and efficient manner.
- Regulation SCI does not require a particular:
  - frequency for performing capacity stress tests; or
  - trigger for performing capacity stress tests.
- Regulation SCI *prescribes* performing a careful risk-based assessment of SCI systems to determine **when** to stress test SCI systems.

Current related ISE policies and procedures:

1. ISE Capacity Planning Policy

CIRAS: Systems Development and Testing Methodology

- Regulation SCI considers the systems development and testing methodology to be a **core** part of the systems development for any SCI system.
- ISE must establish a program to **review and keep current** its systems development and testing methodology for SCI systems and indirect SCI systems.
- Failure to establish such a program would undermine ISE's ability to assess the capacity, integrity, resiliency, availability and security of its SCI systems and indirect SCI systems, as required.

Current related ISE policies and procedures:

1. Development and Automation Services – Software Development Methodology
2. Software Quality Management Procedures
3. ISE Information Security Policy

CIRAS: Systems Development and Testing Methodology – SEC Suggested Criteria

The SEC has identified several criteria that ISE may consider in complying with the systems development and testing methodology requirement:

- Whether ISE identifies and corrects problems detected in the development and testing stages.
- Whether development and test environments are segregated from SCI systems in production.
- Whether ISE personnel have adequately segregated roles between the development and/or test environment, and the production environment.
- How closely the testing environment simulates its production environment.
- Whether ISE verifies change implementation in the production stage.

CIRAS: Regular Reviews and Testing of SCI Systems and Indirect SCI Systems (incl. backup systems)

Purpose: To identify vulnerabilities pertaining to internal or external threats, physical hazards, and natural or manmade disasters.

- Manner and frequency of reviews and testing is at ISE's discretion.
- SEC suggested testing examples:
    a. Reviews of software and systems architecture and design to assess whether they have flaws or dependencies that constitute structural risks that could pose a threat to SCI systems' operational capability.
    b. Inspections of ISE's physical premises can assess some of the vulnerabilities such as physical hazards.
    c. Engaging personnel independent of the team that designed and developed the systems in testing, or employing a process audit role.

Utility Company Systems. Although not SCI systems, ISE should be aware of how issues relating to utility company systems can impact ISE's obligations under Regulation SCI and address such in policies and procedures.

Current related ISE policies and procedures:

1. Fire Safety and Emergency Action Plan
2. ISE Standard: Corporate Physical Security
3. ISE Standard: Non-Employee and Visitor Access
4. ISE Information Security Policy
5. Procedure: Vulnerability Scanning and Patch Management

CIRAS: Business Continuity and Disaster Recovery Plans

ISE must maintain geographically diverse back-up and recovery capabilities.

- The precise nature and location of the backup site is at ISE's discretion (no minimum distance required).
- Site location can be based on the particular vulnerabilities associated with the site and the nature, size, technology, business model, and other aspects of ISE's business.
- Should be a *significant* distance away from the primary site, or otherwise address the risk that a wide-scale disruption could impact either or both of the sites and its labor pool.
- But should not be so distant from the primary facility that ISE may not rely primarily on the same labor pool to staff both facilities if it believes it to be appropriate.
- Should not rely on the same infrastructure components *(e.g.*, transportation, telecommunications, water supply, and electric power).

Backup systems are not required to be identical (*e.g.*, same speed and efficiency) to the primary facility.

- Members are not required to use the backup facility in the same way they use the primary facility.
- Members are not required to co-locate their systems at backup sites to replicate the speed and efficiency of the primary site.

ISE has critical SCI systems subject to a two-hour recovery goal.

- ISE's critical SCI systems are SCI systems that directly support functionality relating to its foreign currency options (*i.e.*, exclusively listed securities under Regulation SCI).

CIRAS: Business Continuity and Disaster Recovery Plans – Resumption Requirements

Next Day Resumption of Trading, and Two-Hour Resumption of Critical SCI Systems Following a Wide-Scale Disruption

- Recovery timeframes are concrete *goals* and the *standards* against which the reasonableness of ISE's BC/DR plans will be assessed by the SEC and its inspection staff.
- The resumption requirement is not dependent on the time of day that the loss of functionality occurs, although the SEC acknowledges that the time of day of a disruption can affect actual recovery times.
- A hard and fast resumption timeframe may not be achievable in each and every case, given the variety of disruptions that potentially could arise and pose challenges even for well-designed BC/DR plans.

Two-Hour Resumption Goal: Critical SCI Systems Only

- Design BC/DR plans that contemplate resumption of critical SCI system functionality to meet a recovery goal of two hours, or less.

Next Business Day Resumption of Trading: SCI Systems

- Systems that directly support trading, order routing, and market data would be subject to the next-business day resumption goal, *unless* they are also critical SCI systems, in which case, they would be subject to the two-hour resumption goal.

CIRAS: Business Continuity and Disaster Recovery Plans – Resumption Requirements (*Cont'd*)

Exception for Market Regulation and/or Market Surveillance Systems

- Not held to resumption goals *unless* they are also critical SCI systems *(i.e.*, currently ISE market regulation and/or market surveillance systems used to regulate and/or surveil ISE foreign currency options).
- The resumption of trading and critical SCI systems could occur following a wide-scale disruption *without* the immediate availability of market regulation and/or market surveillance systems (*unless* they are also critical SCI systems).

Current related ISE policies and procedures:

1. Business Continuity Management Program Strategy
2. ISE Disaster Recovery Plan
3. Business Continuity / Disaster Recovery Test Schedule
4. Various Regulation SCI-related business-level Business Continuity Plans

CIRAS: Systems Involved in the Collection, Processing, and Dissemination of Market Data

- Establish standards that result in SCI systems and indirect SCI systems being designed, developed, tested, maintained, operated, and surveilled in a manner that facilitates the successful collection, processing, and dissemination of market data.
- The accurate, timely, and efficient processing of data is important to the proper functioning of the securities markets and it is important that ISE's market data systems are reasonably designed to maintain market integrity.

Market Data

- Not intended to include only consolidated market data, but proprietary market data as well.
- ISE SCI systems directly supporting proprietary market data or consolidated market data are subject to this rule.
- Consolidated feeds broadly distribute ISE trade and quote data to the public.
- Monitor the speed of proprietary feeds compared to data transmission to the consolidated feeds to ensure that market data is not being sent to proprietary customers **before** sending such data to the consolidated feeds.

Current related ISE policies and procedures:

1. Development and Automation Services – Software Development Methodology
2. Software Quality Management Procedures Document
3. ISE Capacity Planning

CIRAS: Monitoring of SCI Systems and Indirect SCI Systems

- SCI systems and indirect SCI systems must be monitored to identify *potential* SCI events.
- Monitoring process should be able to identify systems problems as a matter of standard operations.
- ISE maintains flexibility to establish parameters that define the types of systems problems to which technology personnel should be alert, as well as the frequency and duration of monitoring.
- Monitoring in tandem with escalation to responsible SCI personnel helps ensure Regulation SCI compliance.
- ISE must have policies and procedures to identify, designate, and escalate potential SCI events to responsible SCI personnel.

Current related ISE policies and procedures:

1. ISE Incident Management Policy & Process Document
2. Application Support/Operations – Tool Inventory List
3. Surveillance Procedures Manual (Reg SCI Compliance Section)
4. Policy: Information Security Management
5. Regulation SCI – Systems Compliance Policy and Procedures
6. ISE Information Security Policy

SYSTEMS COMPLIANCE – SCI Systems

ISE SCI systems must operate in a manner that complies with the Exchange Act, the rules and regulations thereunder, and ISE's rules. To help accomplish this:

- ISE must test all SCI systems and any changes to SCI systems prior to implementation.
- ISE must have a system of internal controls over changes to SCI systems.
- ISE must have a plan for assessments of the functionality of SCI systems designed to detect systems compliance issues, including by responsible SCI personnel and by personnel familiar with applicable provisions of the Exchange Act (*e.g.*, legal) and the rules and regulations thereunder and ISE's rules and governing documents, as applicable.
- ISE must have a plan of coordination and communication between regulatory and other personnel of ISE, including by responsible SCI personnel, regarding SCI systems design, changes, testing, and controls designed to detect and prevent compliance issues.

SYSTEMS COMPLIANCE – Pre-Implementation Testing

- ISE must test all SCI systems and any changes to SCI systems prior to implementation.
- ISE must have a system of internal controls over changes to SCI systems.
- ISE should consider, on an ongoing basis, whether its policies and procedures should provide for testing of certain systems changes **after** their implementation, to ensure that the systems changes operate in compliance with the Exchange Act and relevant rules.
- ISE should also consider, on an ongoing basis, whether its policies and procedures are reasonably designed.

Why Pre-Implementation Testing?

- Helps ISE identify *potential* problems **before** such problems have the ability to impact markets and investors.
- Helps ISE identify *potential* compliance issues **before** new systems or systems changes are implemented.

Current related ISE policies and procedures:

1. Software Quality Management Procedures Document
2. ISE Information Security Policy

SYSTEMS COMPLIANCE – Internal Controls

- Helps ISE identify and resolve *potential* compliance issues **before** system changes are implemented.
- Ongoing monitoring of systems functionality helps prevent SCI systems from becoming noncompliant resulting from, *e.g.*, inattention or failure to review compliance with written policies and procedures.

Internal Controls Examples:

- Communication and cooperation between legal, business, technology, and compliance departments of ISE.
- Appropriate authorization of systems changes by relevant departments *prior to* implementation.
- Review of systems changes by legal or compliance departments prior to implementation.
- Monitoring of systems changes *after* implementation.

Current related ISE policies and procedures:

1. ISE Change Management Policy & Process Document
2. Information Security Program Plan
3. Rule Change Process Document
4. ISE Information Security Policy

SYSTEMS COMPLIANCE – Assessment of SCI System Functionality to Detect Compliance Issues

- ISE has discretion in determining the manner and frequency of assessments.
- Conducted by:
  - responsible SCI personnel; and
  - personnel familiar with applicable provisions of the Exchange Act, its rules and regulations and ISE's rules and governing documents.
- The range of factors that may impact the nature and frequency of assessments include ISE's:
  - governance structure,
  - business lines, and
  - legal and compliance framework.
- ISE's plan for assessments could include, *e.g.*:
  - a plan for monitoring,
  - a plan for testing or assessments, as appropriate, at a frequency (*e.g.*, periodic or continuous) that is based on ISE's risk assessment of each SCI system, and
  - independent validation under certain circumstances.

Current related ISE policies and procedures:

1. Regulation SCI – Systems Compliance Policy & Procedures

SYSTEMS COMPLIANCE – Coordination and Communication regarding SCI Systems

- Establish a plan of coordination and communication about SCI systems design, changes, testing, and controls designed to detect and prevent systems compliance issues.
- Coordination and communication between:
  - regulatory and other personnel of ISE, including by responsible SCI personnel, and
  - information technology and regulatory staff
- Helps ensure that ISE's business interests do not undermine regulatory, surveillance, and compliance functions and, more broadly, the requirements of the Exchange Act, during the development, testing, implementation, and operation processes for SCI systems.

Current related ISE policies and procedures:

1. Rule Change Process Document

SYSTEMS COMPLIANCE – Safe Harbor (Overview)

ISE staff are liable for aiding and abetting or causing a violation of Regulation SCI by ISE.

- ISE staff includes contractors, consultants, and other non-employees used by ISE in connection with its SCI systems.

Individual Safe Harbor – Systems Compliance (Rule 1001(b)**) Only.**

- Regulation SCI provides a safe harbor from liability, subject to certain conditions, to ISE staff.
- The Individual Safe Harbor rule has two prongs:
  - the first applies to <u>all</u> ISE staff; and
  - the second imposes additional criteria on those ISE staff responsible, or having supervisory responsibility, for an SCI system *before* they can rely on the Individual Safe Harbor.
- ISE Staff will not have aided, abetted, counseled, commanded, caused, induced, or procured the violation by ISE of Rule 1001(b) if he/she:
  - has **reasonably discharged** his/her duties and obligations in accordance with ISE's policies and procedures; and
  - was **without reasonable cause to believe** that ISE's policies and procedures relating to an SCI system for which he/she was responsible, or had supervisory responsibility, were not established, maintained, or enforced in accordance with Rule 1001(b), in any material respect.
- The **burden of proof** is on the ISE staff seeking the Individual Safe Harbor.
- The occurrence of a systems compliance issue in and of itself generally does not impose liability.

SYSTEMS COMPLIANCE – Safe Harbor Protection

ISE Staff who are not responsible for, *AND* do not have supervisory responsibility over, SCI Systems.

- Applies to all ISE staff
- Can qualify for the Individual Safe Harbor, *regardless of their belief* regarding the reasonableness of ISE's systems compliance policies and procedures.
- Not "deputized to police" the actions of other ISE staff.
- Would not be liable even if ISE itself did not have reasonably designed systems compliance policies and procedures or did not enforce its policies and procedures, **as long as** he/she *discharged his/her duties and obligations* under the policies and procedures in a *reasonable manner*.

ISE Staff who are responsible for, *OR* have supervisory responsibility over, SCI Systems.

- In addition to the above, a higher burden is imposed on ISE staff who are responsible for SCI systems and ISE staff with supervisory responsibility over others' activities related to an SCI system.
  - He/she likely already has the responsibility to supervise others' activities related to a particular SCI system.
  - He/she would already have information to form a reasonable belief regarding the reasonableness of the policies and procedures.
- Upon becoming aware of *potential* **material non-compliance** of ISE's policies and procedures related to an SCI system, he/she should take action to:
  - review and address, or
  - direct other personnel to review and address, such material non-compliance.
- Required to be knowledgeable about ISE's systems compliance policies and procedures and should be trained in such systems compliance policies and procedures.

Incident Management Escalation Procedures for Potential SCI Events*

- All ISE staff must immediately escalate systems issues, as applicable to incident managers:
  - Level 1 Manager (disruption)
  - Security Operations Manager (intrusion)
  - Product Management Group (compliance issue)
- Incident managers determine whether affected system is an SCI system (see SCI systems list) or an indirect SCI system (clear with Tim Kropp).
- Begin incident troubleshooting/corrective action until resolved.
- If an SCI system or indirect system, incident managers escalate to responsible SCI personnel.
- Responsible SCI personnel (**only**) declare whether incident is also an SCI event.
  - If it is an SCI event, the SEC and ISE members will be notified, subject to certain exceptions.
- Maintain an internal record of all documents related to the SCI event in accordance with ISE's record retention policy.

***SEE INCIDENT ESCALATION FLOW CHARTS IN J:\REGULATION SCI**

Incident Management Escalation Procedures – Current Related ISE Policies and Procedures

The following policies and procedures relate to incident management at ISE:

- *ISE Incident Management Policy & Process Document*
  - Owner: Joe Alfano
  - Generally applicable to systems disruptions
- *Policy: Information Security Incident Management*
  - Owner: Tim Kropp
  - Generally applicable to systems intrusions
- *Regulation SCI – Systems Compliance Policy and Procedures*
  - Owner: Claire McGrath
  - Generally applicable to systems compliance issues
- *Surveillance Procedures Manual (Regulation SCI Compliance* Section*)*
  - Owner: Russ Davidson
  - Generally applicable to market surveillance systems

REGULATION SCI RESOURCES

Additional Regulation SCI Resources can be found at: **J:\Regulation SCI.** These include, but are not limited to:

- Regulation SCI Compliance Manual
- Current List of SCI Systems
- Toolkit
- SEC Knowledge Chest
- Training Materials

QUESTIONS?

Contact ISE Compliance Officer

Claire McGrath

x2130