FOR INTERNAL USE ONLY

INTERNATIONAL SECURITIES EXCHANGE. ISE GEMINI.

Regulation Systems Compliance & Integrity Compliance Manual

Effective Date: November 3, 2015 (FINAL)

ISE Compliance Department

11-3-2015

Version 1.0

REVISION HISTORY

DATE	SECTION	BRIEF DESCRIPTION	VERSION NUMBER	OWNER
11/3/2015	N/A	Original Document	1.0	Claire McGrath, Compliance Officer

Table of Contents

I. EXECUTIVE SUMMARY

On November 19, 2014, the U.S. Securities and Exchange Commission (**Commission**) adopted Regulation Systems Compliance and Integrity[1] (**Regulation SCI**) under the Securities Exchange Act of 1934 (**Exchange Act** or **Act**).[2] Regulation SCI became effective on February 3, 2015 (**Effective Date**) with a compliance date of nine (9) months after the Effective Date, or November 3, 2015 (**Compliance Date**), subject to limited exception.[3]

Regulation SCI applies to certain self-regulatory organizations (including registered clearing agencies), alternative trading systems, plan processors, and exempt clearing agencies (collectively, **SCI Entities**[4]) and requires these SCI Entities to comply with requirements with respect to the automated systems central to the performance of their regulated activities.[5]

It is the Commission's belief that the adoption of, and compliance by SCI Entities with, Regulation SCI will advance 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, as well as reinforce the requirement that such systems operate in compliance with the Exchange Act and rules and regulations thereunder, thus strengthening the infrastructure of the U.S. securities markets and improving its resilience when technological issues arise. In this respect, Regulation SCI establishes an updated and formalized regulatory framework, thereby helping to ensure more effective Commission oversight of such systems.[6]

The International Securities Exchange LLC (**ISE LLC**), ISE Gemini LLC (**ISE Gemini**), and ISE Mercury LLC[7] (**ISE Mercury**) (collectively referred to hereinafter as, **ISE**), as self-regulatory organizations, are SCI Entities and thus subject to the requirements of Regulation SCI.

ISE has established, and will maintain and enforce, this Regulation SCI Compliance Manual, which is applicable to all ISE employees and consultants (collectively, **ISE Staff**), to ensure that ISE is, and continues to be, compliant with the requirements of Regulation SCI.

- **Policy Owner:** ISE Compliance Officer
- **Legal/Regulatory Framework:** Regulation Systems Compliance and Integrity; Securities Exchange Act of 1934.
- **Audience/Applicability:** This Regulation SCI Compliance Manual applies to all ISE Staff.

---

[1] *17 CFR 242.1000-1007*

[2] Securities Exchange Act Release No. 34-73639 (Nov. 19, 2014) 79 FR 72252 (December 5, 2014), available at: www.sec.gov (**Adopting Release**).

[3] As discussed in *Business Continuity and Disaster Recovery Plan Testing*, below, the Commission has a later compliance date for testing of SCI Entity business continuity / disaster recovery plans of twenty-one (21) months after the Effective Date, or November 2, 2016 (**BC/DR Testing Compliance Date**). The compliance date for industry-sector-wide testing is November 2, 2017 (**Industry- Sector-Wide BC/R Testing Compliance Date**).

[4] SCI Entities are discussed in *SCI Entities*, below.

[5] See Adopting Release at p. 1.

[6] See Adopting Release at pp. 18-19.

[7] ISE Mercury is currently pending Commission approval.

- **Revisions and Approvals:** Revisions to the Regulation SCI Compliance Manual are limited to the ISE Compliance Officer and his/her designee. All revisions must be authorized and approved by the ISE Compliance Officer before they take effect.

- **Document Retention Requirement:** 5 years.[8]

- **Regulation SCI Repository/Recordkeeping:** The Compliance Department maintains copies of all Regulation SCI related documents in the **Compliance folder** on the **Legal shared drive**. The Compliance folder is not accessible to ISE staff at large. Instead, the Compliance Department also maintains a **Regulation SCI folder** on the **J Drive** that is accessible by all ISE staff. The Regulation SCI folder on the J Drive houses the information necessary for ISE's Staff to understand ISE's Regulation SCI compliance program and includes related ISE policies and procedures, Regulation SCI's adopting release, Form SCI, various templates, Regulation SCI cheat sheets, and this *Regulation SCI Compliance Manual*, among other documents.

- **Related ISE Policies and Procedures:**
  - *Addendum to ISE Incident and Crisis Escalation Process*
  - *Application Support/Operations – Tool Inventory List*
  - *Business Continuity / Disaster Recovery Test Schedule*
  - *Business Continuity Management Program Strategy*
  - *Business Continuity Plan for Application Support*
  - *Business Continuity Plan for Capacity Planning*
  - *Business Continuity Plan for Compliance Office*
  - *Business Continuity Plan for Corporate Sourcing and Vendor Management Office*
  - *Business Continuity Plan for Facilities*
  - *Business Continuity Plan for ISE/ISE Gemini/ISE Mercury Surveillance*
  - *Business Continuity Plan for ISE Market Data*
  - *Business Continuity Plan for Legal*
  - *Business Continuity Plan for Market Operations*
  - *Business Continuity Plan for Network Services*
  - *Business Continuity Plan for Product Management*
  - *Business Continuity Plan for Project Management Office (PMO)*
  - *Business Continuity Plan for Software Quality Management (SQM)*
  - *Business Continuity Plan for Systems & Storage Management and Infrastructure Engineering*
  - *Business Continuity Plan for Technology Member Services (TMS)*
  - *Development and Automation Services – Software Development Methodology*
  - *Fire Safety and Emergency Action Plan*
  - *Information Security [ ] Program Plan*
  - *Internal Audit Charter – Deutsche Börse Group Policy Statement (11 June 2015)*
  - *ISE Capacity Planning*
  - *ISE Change Management Policy & Process Document*
  - *ISE Disaster Recovery Plan*
  - *ISE Incident and Crisis Escalation Process*
  - *ISE Incident Management Policy & Process Document*

[8] See *Record Retention Policy* which can be found in the *ISE Code of Business Conduct and Ethics*.

- *ISE Information Security Policy*
- *ISE Information Security Program Roles and Responsibilities*
- *ISE Problem Management Policy & Process Document*
- *ISE Standard: Corporate Physical Security*
- *ISE Standard: Non-Employee and Visitor Access*
- *Policy: Information Security Incident Management*
- *Policy: Third Party Providers of SCI Systems – Exegy*
- *Procedure: Vulnerability Scanning & Patch Management*
- *Record Retention Policy* (see ISE Code of Business Conduct and Ethics)
- *Regulation SCI: Annual Review Program – Internal Audit Approach*
- *Regulation SCI – Systems Compliance Policy & Procedures*
- *Rule Change Process Document*
- *Software Quality Management Procedures Document*
- *Standard – Indirect SCI Systems*
- *Surveillance Procedures Manual (Reg SCI Compliance Section)*

- **Other Referenced Third Party Documents:**
  - Exegy, Inc.:
    - *Exegy Ticker Plant Lease*, dated June 28, 2011
    - Various Exegy Regulation SCI Polices (*see* **Appendix F-2: THIRD PARTY – Exegy Regulation SCI Policies and Procedures Pursuant to ISE *Policy: Third Party Providers of SCI Systems – Exegy***)
  - FINRA:
    - *Framework for Managing SCI Workflow under RSAs* term sheet
    - Various FINRA Regulation SCI Policies (*see* **Appendix F-1: THIRD PARTY – FINRA Regulation SCI Policies and Procedures**)

INTENTIONALLY LEFT BLANK

II. OVERVIEW

Regulation SCI imposes certain obligations and duties upon ISE. As further described herein, these obligations and duties include, among other things:

- Establishing, maintaining, and enforcing written policies and procedures reasonably designed to ensure that certain systems have levels of capacity, integrity, resiliency, availability, and security adequate to maintain ISE'S operational capability and promote the maintenance of fair and orderly markets;

- Establishing, maintaining, and enforcing written policies and procedures reasonably designed to ensure that certain systems operate in a manner that complies with the Act and the rules and regulations thereunder and ISE's own rules;

- Taking corrective action with respect to SCI Events[9] to mitigate potential harm to investors and market integrity resulting from such event and devoting sufficient sources to remedy the event as soon as reasonably practicable;

- Notifying the Commission about the occurrence of an SCI Event and disseminating information about certain SCI Events to affected, or all, members of ISE, as applicable;

- Maintaining backup and disaster recovery capabilities sufficiently resilient and geographically diverse and that are reasonably designed to achieve next business day resumption of trading and two-hour resumption of Critical SCI systems[10] following a wide-scale disruption;

- Effectively managing, and notifying the Commission of, material changes to any SCI Systems;[11]

- Conducting periodic reviews (not less than once each calendar year) of ISE's compliance with Regulation SCI by objective, qualified personnel and submitting such SCI review reports to ISE's senior management, the Commission, and ISE's Board of Directors;

- Mandating participation by designated members or participants in scheduled functional and performance testing of the operation of ISE's business continuity and disaster recovery plans, including backup systems, and coordinating such testing on an industry- or sector-wide basis with other SCI Entities;

- Recordkeeping obligations for all documents relating to compliance with Regulation SCI, including records prepared or maintained by a service bureau or other recordkeeping service; and

[9] SCI Events are described in *SCI Events*, below.
[10] Critical SCI Systems are described in *Critical SCI Systems*, below.
[11] SCI Systems are described in *SCI Systems,* below.

- Filing Form SCI with the Commission.

It is ISE's policy that all ISE Staff are required to perform their duties in compliance with this Regulation SCI Compliance Manual, as well as related policies and procedures, as applicable.

A. TRAINING

All ISE Staff must understand their duties and obligations under ISE's policies and procedures in order to reasonably discharge such duties and obligations.[12] This will be accomplished through Regulation SCI General Awareness Training.

Further, ISE Staff who have responsibility for an SCI System, or who have supervisory responsibility over others' activities related to SCI System(s), must be knowledgeable about ISE's Systems Compliance policies and procedures.[13] This will be accomplished through targeted Regulation SCI Systems Compliance Training.

The above training is necessary to ensure that ISE Staff are knowledgeable about their responsibilities so that they can properly discharge them and be covered by Regulation SCI's safe harbor from individual liability with regards to systems compliance, as described in *Systems Compliance Safe Harbor from Liability for Individuals: Rule 1001(b)(4)*, below.

1. REGULATION SCI GENERAL AWARENESS TRAINING

Consistent with the guidance in the Adopting Release, ISE Staff shall undergo annual Regulation SCI General Awareness Training. This training will be provided by the ISE Compliance Officer. Regulation SCI General Awareness Training will be evidenced by attendance sheets and/or certificates of completion. The method of delivery is at the discretion of the ISE Compliance Officer.

2. REGULATION SCI SYSTEMS COMPLIANCE TRAINING

Additionally, ISE departments subject to specific SCI Systems Compliance policies and procedures shall also undergo annual business-specific Systems Compliance Training (given by the business) to ensure that ISE Staff in those departments understand the requirements of those policies and their duties and obligations thereunder. Systems Compliance Training will be evidenced by attendance sheets and/or certificates of completion. The method of delivery is at the discretion of the relevant department(s).

INTENTIONALLY LEFT BLANK

[12] See Adopting Release at p. 236, footnote 728.
[13] See Adopting Release at p. 235.

III. SCI ENTITIES

Regulation SCI Rule (hereafter, **Rule ___**) 1000, *Definitions*,[14] defines SCI Entity as an SCI self-regulatory organization (**SCI SRO**), SCI alternative trading system, plan processor, or exempt clearing agency subject to ARP.[15]

SCI SRO is defined in Rule 1000, *Definitions*, as any national securities exchange, registered securities association,[16] or registered clearing agency, or the Municipal Securities Rulemaking Board; provided however, that for purposes of this section, the term SCI self-regulatory organization shall not include an exchange that is notice registered with the Commission pursuant to 15 U.S.C. 78f(g) or a limited purpose national securities association registered with the Commission pursuant to 15 U.S.C. 78o-3(k).

The Commission has named the International Securities Exchange LLC and ISE Gemini LLC, both registered national securities exchanges,[17] as SCI Entities.[18] It should be noted here that ISE Mercury, when approved by the Commission and operational, will also be an SCI SRO and, thus, an SCI Entity subject to Regulation SCI.

Each of the identified categories of entities plays a significant role in the U.S. securities markets and/or has the potential to impact investors, the overall market, or the trading of individual securities.[19]

INTENTIONALLY LEFT BLANK

[14] See **Appendix I: Regulation SCI Rules 1000 – 1007**, as a reference guide for all Regulation SCI rules mentioned hereafter.
[15] ARP means Automation Review Policy. ARP has been superseded and replaced by Regulation SCI, with regards to SCI Entities. See Adopting Release at p. 2.
[16] The Commission has identified the Financial Industry Regulatory Authority (**FINRA**) as the only registered national securities association. See Adopting Release at p. 27. As described in *SCI Systems*, below, FINRA is a 3rd party provider of an SCI System (market surveillance) for ISE.
[17] See Adopting Release, at pp. 31-32, footnote (**FN**) 74 at p. 32.
[18] The terms SCI Entity or SCI Entities shall be understood to include both ISE and ISE Gemini, as well as ISE Mercury when it is operational, at all times, whether used in this document or in any of the Related Documents referenced in *Executive Summary*, above.
[19] See Adopting Release at p. 30.

IV. SCI SYSTEMS, CRITICAL SCI SYSTEMS, and INDIRECT SCI SYSTEMS

The primary focus of Regulation SCI is to ensure that certain systems of SCI Entities, referred to as SCI Systems, maintain levels of capacity, integrity, resiliency, availability, and security adequate to maintain their operational capability and promote the maintenance of fair and orderly markets, as well as operate in a manner that complies with the Exchange Act.

As further described in the following sections, there are three broad categories of systems subject to Regulation SCI (collectively, **SCI Systems**): SCI Systems, Critical SCI Systems and Indirect SCI Systems.

- **SCI Systems** are subject to all provisions of Regulation SCI, except for certain requirements applicable only to Critical SCI Systems.
- **Critical SCI Systems** are a subset of SCI Systems that are subject to certain heightened resilience and information dissemination provisions of Regulation SCI.
- **Indirect SCI Systems** are subject only to the provisions of Regulation SCI relating to security and intrusions.[20]

A Note on SCI Systems Operated By Third Parties on ISE's Behalf. Although ISE may determine to contract with third parties to operate SCI Systems on its behalf, ISE is responsible for having in place processes and requirements to ensure that it is able to satisfy the requirements of Regulation SCI for SCI Systems operated on its behalf by a third party. This can be accomplished through appropriate due diligence, contract terms, monitoring, or other methods.[21] The Commission has stated, in its Regulation SCI Frequently Asked Questions[22] (**Regulation SCI FAQs**) that the expertise and access of the third party directly operating the applicable SCI System could be reasonably leveraged by the SCI Entity on whose behalf that system is being operated in fulfilling regulatory obligations under Regulation SCI. As described in *SCI Systems*, below, ISE utilizes the services of two (2) third parties: (i) Exegy, Inc., with respect to trading systems (see, in particular, *ISE SCI Systems – Trading Systems*, below); and (ii) FINRA, with respect to market surveillance (see, in particular, *ISE SCI Systems – Market Surveillance*, below). The *ISE Information Security Policy* documents ISE's Third Party Service Delivery Management policy, the objective of which is to implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements. Refer to the *ISE Information Security Policy* for details.

- **EXEGY, INC.:** ISE's *Policy: Third Party Providers of SCI Systems – Exegy* documents the Regulation SCI obligations ISE requires Exegy to comply with as a third party provider of an SCI System to ISE. Refer to **Appendix F-2: THIRD PARTY – Exegy Regulation SCI Policies and Procedures Pursuant to ISE *Policy: Third Party Providers of SCI Systems – Exegy*** for the list of Regulation SCI-related documents submitted to ISE by Exegy, copies of which are stored in the Compliance Department's shared drive.

[20] See Adopting Release at p. 79.
[21] See Adopting Release at p. 93.
[22] See the Commission's Division of Trading and Markets Responses to Frequently Asked Questions Concerning Regulation SCI (**Regulation SCI FAQs**) at: http://www.sec.gov/divisions/marketreg/regulation-sci-faq.shtml

- **FINRA:** Refer to **Appendix F-1: THIRD PARTY – FINRA Regulation SCI Policies and Procedures** for the list of policies and procedures developed by FINRA for Regulation SCI with respect to RSA systems. Copies of FINRA's *Framework for Managing SCI Workflow under RSAs* term sheet as well as FINRA's Regulation SCI Policies and Procedures are stored on the Compliance Department's shared drive.

A. SCI SYSTEMS

Rule 1000, *Definitions*, defines SCI Systems as all computer, network, electronic, technical, automated, or similar systems of, or operated by or on behalf of, an SCI entity that, with respect to securities, directly support:

1) trading,
2) clearance and settlement,[23]
3) order routing,
4) market data,
5) market regulation, or
6) market surveillance.

The Commission has stated that, because systems of SCI Entities are complex and highly interconnected, the definition of SCI Systems "should not exclude functionality or supporting systems on which the [above] six identified categories of systems rely to remain operational."[24]

In addition, the Commission has included in the definition of SCI Systems, systems operated by a third party on behalf of the SCI Entity that directly support one of the six functions listed above. If an SCI Entity utilizes a third party for an applicable SCI System, the SCI Entity is responsible for having in place processes and requirements to ensure that it is able to satisfy the requirements of Regulation SCI for those systems operated on its behalf by a third party.

Currently, ISE systems subject to Regulation SCI are those systems that directly support trading, order routing, market data, market regulation and market surveillance (*i.e.*, five of the six SCI system categories, above). The list of ISE SCI Systems can be found at **Appendix C: SCI Systems**, below. These systems are described in the following sections.

1. ISE SCI SYSTEMS – TRADING SYSTEMS

The following is a description of the ISE systems that directly support trading and have been identified as SCI Systems.

[23] Because ISE is an exchange and not a clearing agency, this category does not apply to ISE SCI Systems.
[24] See Adopting Release at p. 84.

Trading System	Type	Description
Config Client	ISEApps	Manages the configuration settings for parameters used by the ISE Apps.
Exegy	**Third Party**	Exegy Incorporated (**Exegy**) is a third party that provides external market data[25] normalization services on behalf of ISE that directly support ISE's trading systems. These market data normalization services are provided through data feeds that are used in processing external market data through the Exegy Ticker Plants. Exegy Ticker Plants are the hardware appliances that combine commercial off the shelf hardware, Exegy custom hardware accelerator computer boards, and certain Exegy Programs provided to ISE pursuant to the Exegy Agreement. Exegy is the source for member applications to get Equity and OPRA feeds (*e.g.*, EFI)
Exegy Feed Interface (EFI)	Core	Connects to Exegy and subscribes to Equity and OPRA feeds to send the data into the Matching Engine (prices and status). This data is required to open Securities so their instruments can be rotated for trading and lock orders to linkage handlers when the away markets have better prices.
Index Feed Systems (IDS)	ISE Apps	Sends data regarding the status (*e.g.*, open, halted, *etc*.) of the underlying index or foreign currency pair into the Core for the subset of those symbols we list options on.
Market Place Tool (MPT) ***DUPLICATE ENTRY*:** See also, Market Regulation Systems, below.	ISE Apps	Market Operations tool that provides Order and Trade information and Alerts based on member activity as well as an interface to interact with the market (*e.g.*, Post trade adjustments, ABBO management, Quote Puller, Kill Switch). **COMMENT:** This *trading system* has elements of market regulation. *For example*, ABBO management is regulation.
Market Watch (MW) ***DUPLICATE ENTRY*:** See also, Market Regulation Systems, below.	ISE Apps	Market Operations tool that displays all of the instruments listed on the exchanges and their current status. Used at market open to address imbalances. Also provides an interface for market operations to change instrument and Security status (*e.g.*, halt the market). **COMMENT:** This *trading system* has elements of market regulation.

[25] As described in the *Exegy Ticker Plant Lease*, dated June 28, 2011 (hereafter, **Exegy Agreement**), market data means financial information including but not limited to, trade and quote, fundamental, corporate actions and historical information from various financial sources, relating to any of the financial markets supported by Exegy.

Trading System	Type	Description
Market Wide Speed Bump (MWSB) ***DUPLICATE ENTRY*:** See also, Market Regulation Systems, below.	ISE Apps	Monitors market making firms trading activity and triggers an inactivation of their quotes if they exceed predefined risk limit thresholds. **COMMENT:** This *trading system* has elements of market regulation.
Matching Engine (ME)	Core	Monitors the order books to identify matching opportunities applying the appropriate business logic rules for the various order types throughout its processing. Aka: 'The heart of the Core' (*i.e.*, T7).
OCC Trade Reporter (OCCTR)	ISE Apps	Sends trades to the OCC for clearing.
OpCon	Core	Operational interface to the Core for executing operational commands and updating Core configuration settings.
Orderbook Explorer (OBE)	ISE Apps	Market Operations tool that displays instruments listed on the exchanges, their market data and depth on the book. Also provides an interface for Market Operations to cancel/unlock orders.
PostProcesser (POPE)	Core	Houses various Post Processing apps, *e.g.*, Orderbook Server.
Reference Data (Core)	Core	Houses all of the exchanges reference data (*e.g.*, business unit and user information, products and their instruments, market models).
Reference Data Cache External (RDCX)	ISE Apps	Delivers Core Reference data to downstream ISE APPS.
Session Manager	Core	Validates logins and tracks connected users.
System Controller (BOS)	Core	The process that OpCon connects to.
System Monitor	Core	Maintains certain Core operational states and processes operational requests.
Trade Manager (TM)	Core	Captures, manages and publishes Broadcast messages for new Deal Items, Trade Items, and Trades (whether established by the ME or by TM itself due to a Trade Management function).

2. ISE SCI SYSTEMS – ORDER ROUTING

The following is a description of the ISE systems that directly support order routing and have been identified as SCI Systems:

Order Routing System	Type	Description
Gateway / Outbound Feed Interface (GWY/OFI)	Core	Gateway - provides the interface for our DTI members to connect to in order to send orders into our system and

Order Routing System	Type	Description
		Outbound Feed Interface - provides the interface for our Market Operations tools to do the same.
ISE Order Routing System (IORS)	ISE Apps	Provides the FIX interface for members to route orders to our exchanges.
Linkage Order Router (LOR)	ISE Apps	Sends orders that lock with the away better lock to our linkage handlers to route to other exchanges and handle our linkage obligations.
PrecISE	ISE Apps	Order management system that provides a front end interface for trading desks to route and manage orders.
Smart Order Router (SOR)	ISE Apps	Routes the stock legs of combination orders and stock leg allocations that originate at the Matching Engine (ME) and the Trade Manager (TM) to supported stock execution venues and provides the stock execution / allocation data back to the ME and the TM.

a) A Note On Linkage Handlers: Not SCI Systems

Currently, ISE utilizes the services of two third-party routing brokers: Wolverine Execution Services, LLC and Merrill Lynch, Pierce, Fenner & Smith, Inc. (collectively, **Linkage Handlers**). Established in 2013, Linkage Handlers are electronic access members of ISE who have entered into arrangements with ISE to provide routing broker services in accordance with ISE Rule 1903, *Order Routing to Other Exchanges*, and the Options Order Protection and Locked/Crossed Market Plan. Specifically, Linkage Handlers will route certain orders to other exchanges when ISE, for example, is not at the National Best Bid or Offer (**NBBO**) or orders are received that would lock or cross another market. As described below, the systems used by Linkage Handlers to perform their routing broker services for ISE are within the Commission's exception and, therefore, are not SCI Systems subject to Regulation SCI.

The Commission has stated, in its Regulation SCI FAQs, that, as a general matter, systems used for routing orders to other trading centers are within the scope of the definition of SCI Systems. This includes routing orders through one or more third-party routing brokers.[26]

As described in the Regulation SCI FAQs, in determining whether routing systems are, in fact, SCI Systems under Regulation SCI, the system must "directly support" the SCI Entity's order routing functionality. Thus, all systems used by the SCI Entity in the order routing process – up to and including those systems that make the **determination** of which trading center to route a particular order, and the price, size and other characteristics thereof – are systems that "directly support" the order routing of the SCI Entity and, as such, are SCI Systems of the SCI Entity.[27]

Exception (applicable to Linkage Handlers): Commission Staff has stated, in the Regulation SCI FAQs, that those systems that are involved in the delivery of the order to a trading center **after** a routing

[26] See Regulation SCI FAQs at: http://www.sec.gov/divisions/marketreg/regulation-sci-faq.shtml
[27] See Regulation SCI FAQs.

decision is made, and without any ability to alter that routing decision, would generally not be considered SCI Systems of the SCI Entity.[28]

The above-noted Linkage Handlers utilized by ISE do not have the ability to alter a routing decision in the delivery of an order to a trading center after such routing decision is made. ISE and ISE Gemini Rule 1903 provides that the Linkage Handler will receive routing instructions from the Exchange, to route orders to other exchanges and report such executions back to the Exchange. The Linkage Handler cannot change the terms of an order or the routing instructions, nor does the Linkage Handler have any discretion about where to route an order. Therefore, consistent with the Commission Staff's exception, above, Linkage Handlers are not operating SCI Systems on behalf of ISE.

3. ISE SCI SYSTEMS – MARKET DATA

The following is a description of the ISE systems that directly support market data and have been identified as SCI Systems.

Market Data System	Type	Description
Market Data Disseminator (MDD)	Core	Disseminates the various market data feeds to the market data subscribers (ex: Top of book, depth of book etc.).
OPRA Quote/Tape Reporter (OQTR)	ISE Apps	Sends quotes and trades to OPRA.
Reference Data Disseminator (RDD)	Core	Disseminates the reference data feed to its subscribers.

4. ISE SCI SYSTEMS – MARKET REGULATION

The following is a description of the ISE systems that directly support market regulation and have been identified as SCI Systems.

Market Regulation System	Type	Description
Exegy Bridge Service (EBS)	ISE Apps	Provides an operational interface to the Exegy appliance - used for Away BBO management when we have to exclude exchanges from the BBO calculation or if we need to override an Equity status from the Market Operations tools.
Market Place Tool (MPT) ***DUPLICATE ENTRY***: See also, Trading Systems, above.	ISE Apps	Market Operations tool that provides Order and Trade information and Alerts based on member activity as well as an interface to interact with the market (ex: Post trade adjustments, ABBO management, Quote Puller, Kill Switch). **COMMENT:** This *trading system* has elements of market regulation. *For example*, ABBO management is regulation.
Market Watch (MW)	ISE Apps	Market Operations tool that displays all of the instruments listed on the exchanges and their current status. Used at market open to address imbalances. Also provides an

[28] See Regulation SCI FAQs.

Market Regulation System	Type	Description
***DUPLICATE ENTRY*:** See also, Trading Systems, above.		interface for market operations to change instrument and Security status (ex: halt the market). **COMMENT:** This *trading system* has elements of market regulation.
Market Wide Speed Bump (MWSB) ***DUPLICATE ENTRY*:** See also, Trading Systems, above.	ISE Apps	Monitors market making firms trading activity and triggers an inactivation of their quotes if they exceed predefined risk limit thresholds. **COMMENT:** This *trading system* has elements of market regulation.
Real Time Processor (RTP)	ISE Apps	Line readers listen to various streams of data (Matching engine audit trail, LOR audit trail, OPRA data) to be used by plugins downstream. Examples include the Indexer which writes the data to files to be viewed by the Query Viewer tool and processed by MDR plugins for surveillance and reports as well as the Order Writer which writes all of the order information to the Market Place database.

5. ISE SCI SYSTEMS – MARKET SURVEILLANCE

The following is a description of the ISE systems that directly support market surveillance and have been identified as SCI Systems.

Market Surveillance System	Type	Description
Audit Trail server	Core	Saves Matching Engine's audit trail and forwards it to downstream systems. Services replay requests from said systems.
FINRA	**Third Party**	FINRA is a third party that provides market surveillance services pursuant to a Regulatory Services Agreement (**RSA**). Under the RSA, FINRA provides certain surveillance programs, conducted by FINRA, on ISE's behalf.
Surveillance	ISE Apps	Supports Surveillance analysts for monitoring trading practice and regulating ISE's members on the exchange through various alerts and reports.

B. CRITICAL SCI SYSTEMS

Critical SCI Systems are a subset of SCI Systems that, if they were to experience systems issues, would be the most likely to have a widespread and significant impact on the securities markets. As such, Critical SCI Systems are subject to the same provisions as SCI Systems, except that Critical SCI Systems are subject to heightened resilience and information dissemination provisions of Regulation SCI.

Rule 1000, *Definitions*, defines Critical SCI Systems as any SCI Systems of, or operated by or on behalf of, an SCI entity that:

(1) Directly supports functionality relating to:

(i) Clearance and settlement systems of clearing agencies;[29]

(ii) Openings, reopenings, and closings on the primary listing market;[30]

(iii) Trading halts;[31]

(iv) Initial public offerings;[32]

(v) The provision of consolidated market data;[33] or

(vi) Exclusively-listed securities; or

(2) Provide functionality to the securities markets for which the availability of alternatives is significantly limited or nonexistent and without which there would be a material impact on fair and orderly markets.

The definition of Critical SCI System is intended to capture those systems that are critical to the operation of the securities markets, including systems that are potential single points of failure in the securities markets.[34]

1. EXCLUSIVELY-LISTED SECURITIES: RELATED ISE CRITICAL SCI SYSTEMS

ISE has Critical SCI Systems because it has SCI Systems that directly support functionality relating to "exclusively-listed securities."

In the Regulation SCI FAQs,[35] Commission Staff stated that systems that directly support functionality relating to exclusively-listed securities represent single points of failure because exclusively-listed securities, by definition, are listed and traded solely on one exchange and, as such, all trading by market participants in such securities necessarily will be disrupted by a trading disruption or outage on the exclusive listing market.

Commission Staff believes that whether a security is an "exclusively-listed security" for purposes of Regulation SCI depends on the specific facts and circumstances relating to the listing and trading of such security. For example, if a security is subject to an intellectual property or other restriction that expressly

[29] Not applicable. ISE is not a clearing agency.
[30] Not applicable. ISE is not a primary listing market.
[31] Not applicable. See *Trading Halts: No Related ISE Critical SCI Systems*, below, for details.
[32] Not applicable. ISE is an options exchange and, therefore, does not issue initial public offerings (IPOs).
[33] Not applicable. ISE is not a securities information processor (SIP).
[34] See Adopting Release at p. 641
[35] See Regulation SCI FAQs at: http://www.sec.gov/divisions/marketreg/regulation-sci-faq.shtml

limits the listing and trading of the security to a single venue, that security would clearly be an exclusively-listed security for purposes of Regulation SCI.

Based on the Commission's example, above, ISE's Cash-Settled Rate-Modified Foreign Currency Options (**FCOs**), described in *ISE Exclusively-Listed Securities: Cash-Settled Rate-Modified Foreign Currency Options (FCOs)*, below, are (currently[36]) exclusively-listed securities within the meaning of Regulation SCI.

Since neither "exclusively listed securities" and FCOs are "systems," ISE interprets all SCI Systems directly supporting the trading of FCOs as Critical SCI Systems.

For the list of ISE SCI Systems categorized as Critical SCI Systems see **Appendix D: Critical SCI Systems.**

2. ISE EXCLUSIVELY-LISTED SECURITIES: CASH-SETTLED RATE-MODIFIED FOREIGN CURRENCY OPTIONS (FCOS)

Approved for listing and trading in April 2007, ISE currently trades FCOs that include the U.S. dollar on one side of a currency pair and one of ten other currencies such as the Euro, Canadian dollar or Swiss franc on the other side of the pair. The 14 currency pairs trading on ISE are based on the Reuters Composite Currency Rate, as modified by ISE in a way that permits the underlying price of the FCO contract to resemble a price level similar to that of an index option.

Although ISE has sought to protect its innovative rate modification process and other contract terms for FCOs, it has not sought to prohibit the use of the process by other exchanges trading FCOs. ISE has offered, and continues to offer, a license on commercially reasonable terms for the trading of cash-settled rate modified FCOs fungible with the products it trades. Notwithstanding ISE's willingness to license its FCOs, no other exchange is currently trading cash-settled rate-modified FCOs and, as such, ISE's FCOs remain exclusively-listed securities within the meaning of Regulation SCI.

3. TRADING HALTS: NO RELATED ISE CRITICAL SCI SYSTEMS

ISE does not have any **Critical** SCI Systems that effectuate trading halts, as contemplated by Regulation SCI.

With respect to functionality that directly supports "trading halts" as a Critical SCI System, the Regulation SCI FAQs[37] clarify that the term "trading halts," for purposes of this definition, was intended to capture market-wide halts, such as regulatory halts, rather than trading halts on an individual market. It is typically the responsibility of the primary listing market to call such a trading halt. However, those systems used by a trading center to receive such market-wide trading halt communications from the primary listing

[36] The Regulation SCI FAQs also present criteria where, if satisfied, a security subject to an intellectual property or other restriction, may not be considered an exclusively-listed security for purposes of Regulation SCI.
[37] See Regulation SCI FAQs at: http://www.sec.gov/divisions/marketreg/regulation-sci-faq.shtml

market or to implement a trading halt on a particular market would not be considered to be Critical SCI Systems, though they would be SCI Systems[38] under Regulation SCI.

C. INDIRECT SCI SYSTEMS

Rule 1000, *Definitions*, defines Indirect SCI Systems as any systems of, or operated by or on behalf of, ISE that, if breached, would be reasonably likely to pose a security threat to SCI Systems.

Whether a system is "reasonably likely to pose a security threat to SCI Systems" is dependent upon whether that system is effectively physically or logically separated from SCI Systems.[39] Thus, the inquiry into whether any ISE system is an Indirect SCI System will depend on whether it is effectively physically or logically separated from SCI Systems. ISE systems that are adequately physically or logically separated (*i.e.*, isolated from SCI Systems, such that they do not provide vulnerable points of entry into SCI Systems) will not fall within the definition of Indirect SCI Systems.[40]

However, for those SCI Systems where these controls are not present or not reasonably designed, the applicable non-SCI systems would be within the scope of the definition of Indirect SCI Systems and subject to the security standards and Systems Intrusions[41] provisions of Regulation SCI.[42]

Unassailable vs. Assailable Protocols. The primary risk posed by Indirect SCI Systems is that they may serve as vulnerable entry points into SCI Systems.

- **Unassailable protocols** are those that, by design, limit communication to basic network or system diagnostics. They do not provide a mechanism for interacting with system data or permit control of the system at any level. If the protocol that a *potential* Indirect SCI System uses to access the SCI System is "unassailable," it is not reasonably likely that such system would pose a potential vulnerability to ISE's SCI Systems. Thus, implementation, or the existence, of such protocols between potential Indirect SCI Systems and ISE's SCI Systems constitute "reasonably designed and effective controls" that result in adequate separation between the systems.

- **Assailable protocols** are any protocols that can be used to modify SCI Systems or configuration data. Under ISE's Indirect Systems policy (see *Standard – Indirect SCI Systems*) a system will be deemed an Indirect SCI System if: (i) it has a direct connection to an SCI System; and (ii) assailable protocols exist with regards to such system.

[38] For the list of ISE SCI Systems, see *SCI Systems*, above.
[39] See Regulation SCI FAQs at: http://www.sec.gov/divisions/marketreg/regulation-sci-faq.shtml
[40] See Adopting Release at p. 110.
[41] Systems Intrusions are discussed in *Systems Intrusion*, below.
[42] See Adopting Release at p. 111.

The Commission Staff provided the following guidance[43] with respect to what an analysis should consider with regards to whether a system is sufficiently isolated through adequate separation and security controls such that it does not provide vulnerable points of entry into SCI Systems:

- First, ISE will need to identify which of its systems meet the definition of SCI System in Rule 1000, *Definitions*.
- Second, ISE should identify the boundaries of its SCI Systems, and assess which controls or methods of separation are appropriate or necessary to ensure effective physical or logical separation.

- Third, for each SCI System, ISE should consider consulting existing industry standards on logical and physical separation and conform to such standards as appropriate.

Commission Staff has also indicated, in the Regulation SCI FAQs, that if it is *possible* for an SCI System to be accessed, for example, via electronic or physical means by an unauthorized user[44] from a non-SCI System, such non-SCI System would be an Indirect SCI System, and would be subject to certain provisions of Regulation SCI. [Italics added.][45]

1. ISE INDIRECT SCI SYSTEM CRITERIA

ISE participated in the Financial Services Sector Information Sharing and Coordination, Clearing House and Exchange Forum (**CHEF**) working group, the focus of which was formalizing a Regulation SCI Indirect Systems determination process.

In determining whether a non-SCI System is an Indirect SCI System, all ISE computing environments including, but not limited to, Corporate, Development, Quality Assurance, Management, and Trading will be assessed. Adequate controls and risk reduction will entitle systems to be classified as out of scope. The following are categories in which Indirect Systems at ISE *may* exist:

- **Orchestration & Job Scheduling:** Services responsible for, including and not limited to, executing pre-defined scripts and job schedules such as opening and closing the marketplace, end-of-day processing, and facilitating data transfer in and out of SCI Systems. Orchestration and job scheduling are typically considered separate concerns. Both concerns can affect system configuration and are combined for simplicity.

- **Cybersecurity Controls:** Services responsible for, including and not limited to, defending SCI Systems, providing authentication and authorization services, and security information and event monitoring.

[43] See Regulation SCI FAQs at: http://www.sec.gov/divisions/marketreg/regulation-sci-faq.shtml
[44] Such possible unauthorized access would make the SCI System vulnerable to a Systems Intrusion. See discussion of Systems Intrusion at *Systems Intrusion*, below.
[45] See Regulation SCI FAQs.

- **Central Databases and File Shares:** Services responsible for, including and not limited to, access to SCI Systems for data transfer and storage.

- **Jump Hosts, Citrix & Remote Access:** Services responsible for, including and not limited to, access to SCI Systems for administration, market surveillance, computer operations, application operations, network operations, security operations, and market operations.

- **Management:** Services responsible for, including and not limited to, snmp read-write access to SCI Systems, data access (log pulls), alerting, and event management requiring read-write access. For example, snmp read-only would be a non-assailable protocol, for monitoring only, and not in scope.

Consistent with the requirements of Regulation SCI, ISE has documented its methodology for identifying Indirect SCI Systems in the *Standard – Indirect SCI Systems* policy. See also, **Appendix E: Indirect SCI Systems** for examples of ISE Indirect SCI System categories and related application functions.

2. COMMISSION REVIEW

Although the universe of ISE's Indirect SCI Systems is within ISE's control, ISE should reasonably expect Commission Staff to assess its security controls around SCI Systems in connection with an inspection or examination for compliance with Regulation SCI.[46]

INTENTIONALLY LEFT BLANK

[46] See Adopting Release at p. 111.

V. REGULATION SCI POLICIES AND PROCEDURES FOR SCI ENTITIES

Rule 1001, *Obligations related to policies and procedures of SCI entities*, contains the policies and procedures requirements for SCI Entities with respect to:

- Levels of capacity, integrity, resiliency, availability and security of SCI Systems and Indirect SCI Systems – Rule 1001(a);
- Systems Compliance – Rule 1001(b); and
- Identification and designation of Responsible SCI Personnel, and related escalation procedures – Rule 1001(c).

A Note on Regulation SCI Policies and Procedures for Third Parties Operating SCI Systems on Behalf of ISE. Both FINRA and Exegy (third parties) have provided ISE with policies and procedures related to their operation of SCI Systems on behalf of ISE. These policies and procedures are located as follows:

- **FINRA:** The suite of Regulation SCI policies and procedures provided to ISE by FINRA are stored on the Compliance Department's shared drive.
- **EXEGY:** The suite of Regulation SCI policies and procedures provided to ISE by Exegy are stored on the Compliance Department's shared drive.

A. CAPACITY, INTEGRITY, RESILIENCY, AVAILABILITY, AND SECURITY: RULE 1001(a)

Rule 1001(a)(1), *Capacity, integrity, resiliency, availability, and security*, requires that ISE establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its SCI Systems and, for purposes of security standards, Indirect SCI Systems, have levels of capacity, integrity, resiliency, availability, and security, adequate to maintain ISE's operational capability and promote the maintenance of fair and orderly markets.

In order to facilitate compliance with the requirements of Rule 1001(a)(1), Rule 1001(a)(2), *Obligations related to policies and procedures of SCI entities – Capacity, integrity, resiliency, availability, and security*, requires that ISE have certain minimum policies and procedures in place for SCI Systems. Such policies and procedures are subject to ongoing self-assessment.[47]

In particular, Rule 1001(a)(2) requires that ISE establish, maintain, and enforce written policies and procedures for its SCI Systems and, for purposes of security standards, Indirect SCI Systems, which must include, at a minimum, policies and procedures relating to:

1) Reasonable current and future technological infrastructure capacity planning estimates;
2) Periodic capacity stress tests;
3) A program to review and keep current systems development and testing methodology;
4) Regular reviews and testing, as applicable, of such systems, including backup systems;

[47] See Adopting Release at p. 149.

5) Business continuity and disaster recovery plans;
6) Standards that result in such systems being designed, developed, tested, maintained, operated, and surveilled; and
7) Monitoring of such systems to identify potential SCI Events.

The requirements for Rule 1001(a)(2) minimum policies and procedures are described below.

1. Technological Infrastructure Capacity Planning Estimates: Rule 1001(a)(2)(i)

Rule 1001(a)(2)(i), *Obligations related to policies and procedures of SCI entities – Capacity, integrity, resiliency, availability, and security*, requires that ISE establish, maintain, and enforce written policies and procedures for its SCI Systems and, for purposes of security standards, Indirect SCI Systems, that include the establishment of reasonable current and future technological infrastructure capacity planning estimates.

The goal of this minimum policy requirement is to help ISE determine its systems' ability to process transactions in an accurate, timely, and efficient manner and, thereby, help ensure market integrity.[48]

Consistent with the requirements of Rule 1001(a)(2)(i), the *ISE Capacity Planning* policy includes policies and procedures with regards to technological infrastructure capacity planning estimates for SCI Systems and, for purposes of security standards, Indirect SCI Systems. Additionally, the *ISE Information Security Policy* outlines policy with regards to IT infrastructure planning, testing and acceptance focused on advanced planning, testing and preparation to ensure availability of adequate capacity and resources to deliver the required system performance, as well as projections of future capacity requirements to reduce the risk of system overload.

2. Periodic Capacity Stress Tests: Rule 1001(a)(2)(ii)

Rule 1001(a)(2)(ii), *Obligations related to policies and procedures of SCI entities – Capacity, integrity, resiliency, availability, and security*, requires that ISE establish, maintain, and enforce written policies and procedures for its SCI Systems and, for purposes of security standards, Indirect SCI Systems, that include periodic capacity stress tests of such systems to determine their ability to process transactions in an accurate, timely, and efficient manner.

The rule does not prescribe a particular frequency or trigger for stress testing,[49] but stress testing is necessary to help an SCI Entity determine its systems' ability to process transactions in an accurate, timely, and efficient manner.[50]

[48] See Adopting Release at p. 155.
[49] See Adopting Release at p. 157.
[50] See Adopting Release at p. 157, FN 482.

Consistent with the requirements of Rule 1001(a)(2)(ii), the *ISE Capacity Planning* policy includes policies and procedures with regards to periodic capacity stress tests for SCI Systems and, for purposes of security standards, Indirect SCI Systems for purposes of determining system capacity.

3. SYSTEMS DEVELOPMENT AND TESTING METHODOLOGY: RULE 1001(a)(2)(iii)

Rule 1001(a)(2)(iii), *Obligations related to policies and procedures of SCI entities – Capacity, integrity, resiliency, availability, and security*, requires that ISE establish, maintain, and enforce written policies and procedures for its SCI Systems and, for purposes of security standards, Indirect SCI Systems, that include a program to review and keep current systems development and testing methodology for such systems.

An SCI Entity's systems development and testing methodology is a core part of the systems development life cycle for any SCI System.[51] Therefore if ISE did not have a program to review and keep current systems development and testing methodology for SCI Systems, and Indirect SCI Systems, as applicable, its ability to assess the capacity, integrity, reliability, availability and security of its SCI Systems and Indirect SCI Systems, as applicable, would be undermined.[52]

The Commission has identified several criteria that SCI Entities ***may*** consider in complying with Rule 1001(a)(2)(iii):

- how closely the SCI Entity's testing environment simulates its production environment;
- whether the SCI Entity designs, tests, installs, operates, and changes SCI Systems through use of appropriate development, acquisition, and testing controls by ISE and/or its third-party service providers, as applicable;
- whether the SCI Entity identifies and corrects problems detected in the development and testing stages;
- whether the SCI Entity verifies change implementation in the production stage;
- whether development and test environments are segregated from SCI Systems in production; and
- whether the SCI Entity's personnel have adequately segregated roles between the development and/or test environment, and the production environment.[53]

Consistent with the requirements of Rule 1001(a)(2)(iii), the *Development and Automation Services – Software Development Methodology* (**SDM Policy**) includes policies and procedures with regards to the systems development and testing methodology for SCI Systems and, for purposes of security standards, Indirect SCI Systems. The SDM Policy works in tandem with the *Software Quality Management Procedures Document* (**SQM Procedures**) which governs the development of functional test requirements.

[51] See Adopting Release at pp. 158-59.
[52] See Adopting Release at p. 159.
[53] See Adopting Release at p. 159.

Additionally, the *ISE Information Security Policy* includes policies and procedures consistent with the requirements of Rule 1001(a)(2)(iii).

For example:

- The SDM Policy governs the software development life cycle procedures at ISE which is dictated by the following over-arching phases: (i) Idea Conceived; (ii) Requirements Phase; (iii) Design Phase; (iv) Development Phase; (v) Testing Phase; and (vi) Change/Release Management Phase.

- Under the SQM Procedures, two test environments are maintained. One test environment contains the new software version as close to the production environment as possible to facilitate recreating any issues that arise in production. The other test environment is where all new software being tested gets installed.

- The *ISE Information Security Policy* also documents the requirement for production computing and operational facilities (Ops) to be separated from development, testing/infrastructure management (INF) and corporate computing environments to reduce the risk of unauthorized access, malware or changes to the operational system.

- The SQM Procedures also document the procedures the SQM team follows when certifying a release of software from ISE's two primary vendors: Deutche Börse Systems and ISE's internal development group.

- The *ISE Information Security Policy* also documents the general requirement for segregation of duties to reduce opportunities for unauthorized or unintentional modification or misuse of ISE's information assets.

- The *ISE Information Security Policy* includes a policy on Information Systems, Acquisition, Development and Maintenance, the objective of which is the establishment of security requirements for information systems to ensure that security becomes an integral factor, whether the information systems are acquired or developed in-house or whether maintenance is being applied.

4. REGULAR REVIEWS AND TESTING OF SYSTEMS: RULE 1001(a)(2)(iv)

Rule 1001(a)(2)(iv), *Obligations related to policies and procedures of SCI entities – Capacity, integrity, resiliency, availability, and security*, requires that ISE establish, maintain, and enforce written policies and procedures for its SCI Systems and, for purposes of security standards, Indirect SCI Systems, that include regular reviews and testing, as applicable, of such systems, including backup systems, to identify vulnerabilities pertaining to internal and external threats, physical hazards, and natural or manmade disasters.

The rule affords SCI Entities the flexibility to determine an assessment methodology that would be most appropriate for a given system, or a particular functionality of a system.[54] Specifically, the rule requires reviews or testing (or both) to occur, as applicable, so long as the approach is effective to identify vulnerabilities in ISE's SCI Systems, and Indirect SCI Systems, as applicable.[55] For example, although it is unlikely that the systems of utility companies (such as a power company providing general power services for SCI Entities), would be SCI Systems, SCI Entities should be aware of how issues relating to such systems may impact their obligations under Regulation SCI. As such, given the importance of utilities such as the supply of power to the operation of its SCI Systems, an SCI entity should consider whether its policies and procedures should contemplate and address the potential occurrence of SCI Events that arise from the effect of the failure or disruption of such utilities on SCI Systems.[56]

While the rule specifically identifies reviews and testing as a means to identify vulnerabilities pertaining to internal and external threats, physical hazards, and natural or manmade disasters, it does not dictate the precise manner or frequency of reviews and testing, and does not prohibit ISE from determining that there are methods other than reviews and testing that may be effective in identifying vulnerabilities,[57] thereby enabling ISE to determine which method(s) are most appropriate for each SCI System (or Indirect SCI System, as applicable) or particular functionality of a given system, as well as the frequency with which such method(s) should be employed.

For example, ISE may conduct reviews of its 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. Likewise, an inspection of ISE's physical premises may be a method of assessing some of the vulnerabilities listed in the rule (such as physical hazards).[58] Additionally, the rule permits ISE to engage personnel independent of the team that designed and developed the systems in testing, or to employ a process audit role, to comply with this requirement.[59]

Consistent with the requirements of Rule 1001(a)(2)(iv), ISE has developed the following policies and procedures with regards to regular reviews and testing of its SCI Systems and, for purposes of security standards, Indirect SCI Systems: *Fire Safety and Emergency Action Plan*, *ISE Standard: Corporate Physical Security*, *ISE Standard: Non-Employee and Visitor Access, ISE Information Security Policy* and *Procedure: Vulnerability Scanning and Patch Management*.

Further, ISE is a member of the Financial Services Information Sharing and Analysis Center (**FS-ISAC**)[60] and the CyberIntel "working group." ISE regularly participates in cleared events with the Department of Homeland Security (**DHS**), Federal Bureau of Investigations (**FBI**), Secret Service and other agencies where secret level information is exchanged. Currently, several ISE Staff hold clearance and are capable of sitting in on cleared events, and receiving relevant need-to-know information. In addition to the daily information exchange for sector level threat and vulnerability information, ISE regularly receives regular

[54] See Adopting Release at p. 161.
[55] See Adopting Release at pp. 161-62.
[56] See Regulation SCI FAQs at: http://www.sec.gov/divisions/marketreg/regulation-sci-faq.shtml
[57] See Adopting Release at p. 162.
[58] See Adopting Release at p. 163.
[59] See Adopting Release at p. 162, FN 496.
[60] FS-ISAC website: www.fsisac.com.

bulletins from the United States Computer Emergency Readiness Team (**US-CERT**),[61] Microsoft, Redhat, Cisco and other vendors on their products and relevancy to ISE.

5. BUSINESS CONTINUITY AND DISASTER RECOVERY PLANS: RULE 1001(a)(2)(v)

Rule 1001(a)(2)(v), *Obligations related to policies and procedures of SCI entities – Capacity, integrity, resiliency, availability, and security*, requires that ISE establish, maintain, and enforce written policies and procedures for its SCI Systems and, for purposes of security standards, Indirect SCI Systems, that include business continuity and disaster recovery plans that include maintaining backup and recovery capabilities sufficiently resilient and geographically diverse and that are reasonably designed to achieve next business day resumption of trading and two-hour resumption of Critical SCI Systems following a wide-scale disruption.

Geographically Diverse Back Up and Recovery Capabilities: Regulation SCI permits ISE a reasonable degree of flexibility to determine the precise nature and location of its backup site depending on the particular vulnerabilities associated with the site and the nature, size, technology, business model, and other aspects of ISE's business.[62]

While geographic diversity is an important component of every SCI Entity's business continuity and disaster recovery plans (**BC/DR Plans**), a minimum distance for SCI Entities' backup and recovery facilities is not specified by the Commission.[63] However, an SCI Entity with Critical SCI Systems subject to a two-hour recovery goal may find it prudent to establish back-up facilities a significant distance away from the primary sites, or otherwise address the risk that a wide-scale disruption could impact either or both of the sites and their labor pool.[64]

Backup sites should not rely on the same infrastructure components, such as transportation, telecommunications, water supply, and electric power. Notwithstanding, Regulation SCI does not require ISE to have a geographically diverse backup facility 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.[65]

Further, because Rule 1001(a)(2)(v) does not require ISE to require its members or participants to use ISE's backup facility in the same way they use the primary facility (*i.e.*, does not require members or participants to co-locate their systems at backup sites to replicate the speed and efficiency of the primary site), the requirement for geographically diverse backup systems does not mean that the backup systems are required to be identical (*e.g.*, same speed and efficiency) to the primary facility.[66]

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

[61] US-CERT website: www.us-cert.gov.
[62] See Adopting Release at p. 176.
[63] See Adopting Release at pp. 164-65.
[64] See Adopting Release at p. 176, FN 544.
[65] See Adopting Release at p. 176.
[66] See Adopting Release at p. 643.

business continuity and disaster recovery.[67] Thus, "reasonably designed to achieve" means that Regulation SCI's enumerated recovery timeframes are concrete *goals*, consistent with the Interagency White Paper[68] and 2003 BCP Policy Statement[69].[70] As such, the rule's specified recovery timeframes are the *standards* against which the reasonableness of ISE's BC/DR Plans will be assessed by the Commission and its inspection staff.[71]

Moreover, as *recovery goals*, rather than hard and fast deadlines, the enumerated time frames in the rule will continue to allow for ISE to account for the specific facts and circumstances that arise in a given scenario to determine whether it is appropriate to resume a system's operation following a wide-scale disruption.[72]

Because the securities markets are dependent upon the reliable operation of Critical SCI Systems, the Commission believes that it is reasonable to distinguish the two-hour and next-business day recovery goals so that the shorter recovery goal applies to Critical SCI Systems, and the longer recovery goal applies to resumption of trading by non-critical SCI Systems.[73]

- **Two-Hour Resumption Goal:** An SCI entity responsible for a given Critical SCI System will be expected to design BC/DR Plans that contemplate resumption of Critical SCI System functionality to meet a recovery goal of two hours or less.[74] The resumption requirement of this goal is not dependent on the time of day that the loss of functionality occurs, although, consistent with the Interagency White Paper and 2003 BCP Policy Statement, the Commission acknowledges that the time of day of a disruption can affect actual recovery times.[75]

- **Next Business Day Resumption of Trading:** 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. The resumption requirement of this goal is not dependent on the time of day that the loss of functionality occurs, although, consistent with the Interagency White Paper and 2003 BCP Policy Statement, the Commission acknowledges that the time of day of a disruption can affect actual recovery times.[76]

- **Exception for Market Regulation and/or Market Surveillance Systems:** Systems that directly support market regulation and/or market surveillance will not be held to the resumption goals of Rule 1001(a)(2)(v), *Obligations related to policies and procedures of SCI entities – Capacity, integrity, resiliency, availability, and security*, *unless* they are Critical SCI Systems, because the

[67] See Adopting Release at p. 166.
[68] See Interagency Paper on Sound Practices To Strengthen the Resilience of the U.S. Financial System, 68 FR 17809 (April 11, 2003). http://www.gpo.gov/fdsys/pkg/FR-2003-04-11/pdf/03-8896.pdf.
[69] See Business Continuity Planning for Trading Markets, 68 FR 56656 (October 1, 2003). http://www.gpo.gov/fdsys/pkg/FR-2003-10-01/pdf/03-24863.pdf.
[70] See Adopting Release at p. 167.
[71] See Adopting Release at p. 167.
[72] See Adopting Release at p. 167.
[73] See Adopting Release at pp. 169-70.
[74] See Adopting Release at p. 170.
[75] See Adopting Release at p. 171.
[76] See Adopting Release at p. 171.

Commission believes that 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 Critical SCI Systems).[77]

Consistent with the requirements of Rule 1001(a)(2)(v), ISE has developed the following policies and procedures with regards to BC/DR Plans for its SCI Systems and, for purposes of security standards, Indirect SCI Systems: *Business Continuity Management Program Strategy; ISE Disaster Recovery Plan;* and *Business Continuity / Disaster Recovery Test Schedule.* Additionally, ISE's Business Continuity Office maintains business-level Business Continuity Plans (**BCP**) for each department across all business units that are designed to provide immediate response and subsequent recovery from any unplanned business interruption, such as the loss of a critical service (computer processing, telecommunications, etc.), a loss of building access (contamination, etc.), a loss of a critical supplier, or a facility catastrophe (fire, sabotage, etc.). The business-level BCPs most relevant to Regulation SCI are:

- *Business Continuity Plan for Application Support*[78]
- *Business Continuity Plan for Capacity Planning*
- *Business Continuity Plan for Compliance Office*
- *Business Continuity Plan for Corporate Sourcing and Vendor Management Office*
- *Business Continuity Plan for Facilities*[79]
- *Business Continuity Plan for ISE/ISE Gemini/ISE Mercury Surveillance*[80]
- *Business Continuity Plan for ISE Market Data*
- *Business Continuity Plan for Legal*
- *Business Continuity Plan for Market Operations*[81]
- *Business Continuity Plan for Network Services*[82]
- *Business Continuity Plan for Product Management*
- *Business Continuity Plan for Project Management Office (PMO)*
- *Business Continuity Plan for Software Quality Management (SQM)*
- *Business Continuity Plan for Systems & Storage Management and Infrastructure Engineering*[83]
- *Business Continuity Plan for Technology Member Services (TMS)*

6. SYSTEMS DESIGN AND DEVELOPMENT STANDARDS: RULE 1001(a)(2)(vi)

Rule 1001(a)(2)(vi), *Obligations related to policies and procedures of SCI entities – Capacity, integrity, resiliency, availability, and security*, requires that ISE establish, maintain, and enforce written policies and procedures for its SCI Systems and, for purposes of security standards, Indirect SCI Systems, that include standards that result in such systems being designed, developed, tested, maintained, operated, and

[77] See Adopting Release at p. 171.
[78] This BCP is currently categorized as a "mission critical department."
[79] This BCP is currently categorized as a "mission critical department."
[80] This BCP is currently categorized as a "mission critical department."
[81] This BCP is currently categorized as a "mission critical department."
[82] This BCP is currently categorized as a "mission critical department."
[83] This BCP is currently categorized as a "mission critical department."

surveilled in a manner that facilitates the successful collection, processing, and dissemination of market data.

The term "market data" is not intended to include only consolidated market data, but proprietary market data as well and, as such, SCI Systems directly supporting proprietary market data or consolidated market data are subject to Rule 1001(a)(2)(vi). 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.[84] As such, ISE must monitor the speed of its proprietary feeds compared to its data transmission to the consolidated feeds to ensure that it is not improperly sending market data to proprietary customers before sending such data to the consolidated feeds which broadly distribute ISE trade and quote data to the public. See *Transmission of Market Data: Consolidated Feeds vs. Proprietary Feeds*, below, for details on dissemination of market data.

Consistent with the requirements of Rule 1001(a)(2)(vi), the *Development and Automation Services – Software Development Methodology*, *Software Quality Management Procedures Document*, and the *ISE Capacity Planning* policy include policies and procedures with regards to design and development standards for SCI Systems and, for purposes of security standards, Indirect SCI Systems related to collection, processing, and dissemination of market data.

a) Transmission of Market Data: Consolidated Feeds vs. Proprietary Feeds[85]

A Note on Consolidated Market Data. In its January 2010 Market Structure Concept Release, the Commission emphasized the importance of consolidated market data stating that "the public has ready access to a comprehensive, accurate, and reliable source of information for the prices and volume of any national market system (**NMS**) stock at any time during the trading day. This information serves an essential linkage function by helping assure that the public is aware of the best displayed prices for a stock, no matter where they may arise in the national market system." Consolidated market data also plays an important role in price discovery and compliance functions.

Transmission of Market Data: Consolidated Feeds vs. Proprietary Feeds. Regulation NMS Rules 601 and 602 require exchanges to send their best-priced quotes and trade reports to be included in the consolidated feeds. Exchanges are also permitted to distribute customized market data products directly to customers. Regulation NMS Rule 603(a) requires that exchanges distribute market data on terms that are "fair and reasonable" and "not unreasonably discriminatory." As such, this rule prohibits an exchange from releasing data relating to quotes and trades to its customers through **proprietary feeds** *before* it sends its quotes and trade reports for inclusion in the **consolidated feeds**. The disparities in data transmissions that Regulation NMS Rule 603(a) prohibits can have important consequences that risk undermining investor confidence and interfering with the efficiency of the markets. For example:

---

[84] See Adopting Release at p. 178.

[85] Source: "*In the Matter of New York Stock Exchange LLC, and NYSE Euronext*, Respondents. Order Instituting Administrative and Cease-and-Desist Proceedings Pursuant to Sections 19(h)(1) and 21C of the Securities Exchange Act of 1934, Making Findings and Imposing Sanctions and a Cease-And-Desist Order (Sep. 14, 2012)" at http://www.sec.gov/litigation/admin/2012/34-67857.pdf.

- A delay in the release of data to the consolidated feeds in contrast to the proprietary feeds can cause an investor relying on the consolidated feeds to make a trading decision based on a potentially stale picture of current market conditions.

- An exchange's delay in sending its quotes to the consolidated feeds also can cause inefficient execution decisions at other market centers and, under some circumstances, create the appearance of a "crossed" national best bid and offer (**NBBO**), which occurs when the best bid exceeds the best offer. The appearance of a crossed NBBO can cause both uncertainty and the risk of a trade being executed at worse than the best available price.[86]

7. SYSTEMS MONITORING: RULE 1001(a)(2)(vii)

Rule 1001(a)(2)(vii), *Obligations related to policies and procedures of SCI entities – Capacity, integrity, resiliency, availability, and security*, requires that ISE establish, maintain, and enforce written policies and procedures for its SCI Systems and, for purposes of security standards, Indirect SCI Systems, that include monitoring of such systems to identify potential SCI Events.

Rule 1001(a)(2)(vii) seeks to ensure that escalation of a systems problem occurs not only if a systems problem is identified by chance, but that ISE should have a monitoring process in place so that systems problems are identified as a matter of standard operations and pursuant to parameters reasonably established by ISE.[87]

The rule provides ISE with 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.[88]

Escalation to Responsible SCI Personnel: The Commission believes that monitoring in tandem with escalation to Responsible SCI Personnel is an appropriate approach to ensuring SCI compliance.[89] Thus, ISE should have policies and procedures to identify, designate, and escalate potential SCI Events to Responsible SCI Personnel.[90] See *Responsible SCI Personnel*, below, for a description of the integral role Responsible SCI Personnel are required to play in Regulation SCI compliance.

Consistent with the requirements of Rule 1001(a)(2)(vii), it is ISE's policy to incorporate monitoring as part of its incident management processes. For instance, as part of the incident management process for Systems Disruptions documented in the *ISE Incident Management Policy & Process Document*, the Application Support, Network Services and Market Operations groups employ numerous monitoring tools as the primary means of identifying incidents. The list of the tools used can be found in the *Application Support/Operations – Tool Inventory List*.

Examples of the types of activities being monitored by various ISE departments include:

---

[86] A crossed NBBO triggers an exception to the trade-through rule of Regulation NMS. See Regulation NMS Rule 611(b)(4).
[87] See Adopting Release at p. 179.
[88] See Adopting Release at p. 180.
[89] See Adopting Release at p. 180.
[90] See Adopting Release at p. 179.

- Application Support Group:
  - Application process status
  - Errors/exceptions in application logs
  - System resources
  - Market data gaps
  - Performance profile of various systems

- Network Services Group:
  - Network devices and firewall status/availability
  - Member vendor circuits
  - Intersite circuits
  - Market data feeds
  - Infiniband network

- Market Operations Group:
  - Overall market status observed through MarketWatch
  - Obvious errors alerts
  - Order deviation alerts
  - Locked order alerts
  - Market-wide speed bump triggers

- Market Surveillance Department:
  - Monitors for disruptions to the Surveillance System (*i.e.*, the Alert Viewer and the reports found in Citrix) which may include:
    - Data not completed loaded
    - Alerts not running for an extended period of time
  - As documented in the *Surveillance Procedures Manual* (*Reg SCI Compliance* Section), although the Surveillance System falls under the company-wide policies and procedures regarding information security, the Market Surveillance Department also conducts routine checks to confirm that only authorized ISE Staff have access to the Surveillance System and the ISE Technology Department is involved in preventing any unauthorized electronic entry to the Surveillance System

- Information Security Monitoring Activities include:
  - Incident handling
  - Routine scans to detect and prevent unauthorized malicious software
  - Intrusion detection and response
  - Advanced persistent threat and anomaly detection
  - Infrastructure logging
  - Central security logging (**SIEM**)
  - Patch management and vulnerability scanning
  - Jump point / Central access
  - Web access / URL filtering

- Endpoint protection
- Mobile devices, encryption and wireless

- Computer Security Incident Response Team:
  - Proactively monitors indicators such as network monitoring or technology watch functions as part of the Systems Intrusions incident management process documented in the *Policy: Information Security Incident Management*.

With regards to monitoring for Systems Compliance Issues, once ISE SCI Systems are placed into production, there is ongoing and continuous monitoring and testing of the systems to ensure they are operating in accordance with: (i) the Business Requirements Documents;[91] (ii) the intentions of the Technology Development staff, the Product Management Group, the Legal Department and the Market Surveillance staff; and (iii) the Exchange Act, rules and regulations thereunder, and ISE's rules. Departments that may be involved in identifying potential Systems Compliance Issues include:

- The Technology Department;
- Software Quality Management;
- Market Operations;
- The Market Surveillance Department; and
- The Product Management Group.

See the *Regulation SCI – Systems Compliance Policy and Procedures* for details.

Additionally, the *ISE Information Security Policy* outlines monitoring policy for:

- IT Infrastructure Security Management, the objective of which is to secure the protection of information in IT infrastructure which requires careful consideration to dataflow, legal implications, monitoring and protection, including the protection of sensitive information leaving ISE's IT infrastructure and passing through public networks.
- Information Systems Monitoring and Logging, the objective of which is to detect unauthorized information processing activities which requires information systems to be monitored and logged, and information security events to be recorded.

8. Periodic Review of Effectiveness of Rule 1001(a) Policies: Rule 1001(a)(3)

Rule 1001(a)(3), *Obligations related to policies and procedures of SCI entities – Capacity, integrity, resiliency, availability, and security*, requires ISE to periodically review the effectiveness of the policies and procedures required by Rule 1001(a), *Capacity, integrity, resiliency, availability, and security*, and take prompt action to remedy deficiencies in such policies and procedures. As detailed above, these policies govern the following activities applicable to ISE's SCI Systems: (i) reasonable technological infrastructure capacity planning; (ii) periodic capacity stress tests; (iii) systems development and testing methodology; (iv) regular reviews and testing of systems; (v) business continuity and disaster recovery plans; (vi) systems design and development standards; and (vii) systems monitoring.

[91] The Business Requirements Documents (BRDs) are a product of the "Requirements Phase" of ISE's Software Development Life Cycle (SDLC). The development of BRDs should include users, software architects, system engineers, network engineers, and legal department personnel.

The Commission has stated that ISE will not be found to be in violation of this maintenance requirement solely because it failed to identify a deficiency in its policies and procedures immediately after the deficiency occurred if ISE takes *prompt action* to remedy the deficiency once it is discovered, and ISE had otherwise reviewed the effectiveness of its policies and procedures and took prompt action to remedy those deficiencies that were discovered.[92]

Consistent with the requirements of Rule 1001(a)(3), ISE shall review and update its Rule 1001(a) policies and procedures **annually**, the timing of which shall be coordinated by management each year. This management review and update is independent of the audit of the effectiveness of such policies and procedures as described in *Audit of the Effectiveness of Rule 1001 Policies and Procedures*, below.

9. CURRENT SCI INDUSTRY STANDARDS: RULE 1001(a)(4)

Rule 1001(a)(4), *Obligations related to policies and procedures of SCI entities – Capacity, integrity, resiliency, availability, and security*, states that Rule 1001(a) policies and procedures shall be deemed to be reasonably designed if they are consistent with current SCI Industry Standards, which shall be comprised of information technology practices that are widely available to information technology professionals in the financial sector and issued by an authoritative body that is a U.S. governmental entity or agency, association of U.S. governmental entities or agencies, or widely recognized organization. Compliance with such current SCI industry standards, however, shall not be the exclusive means by which to comply with the requirements of Rule 1001(a).

Commission Staff has issued guidance to SCI Entities on developing policies and procedures consistent with current SCI industry standards (**Staff Guidance**).[93] The Staff Guidance lists publications[94] issued by several organizations that cover nine (9) inspection areas, or "domains" relevant to an SCI Entity's systems capacity, integrity, resiliency, availability, and security.[95]

SCI Industry Standards Inspection Areas/Domains		
Audit	Capacity Planning	Information Security and Networking
Outsourcing	Contingency Planning	Systems Development Methodology
Application Controls	Physical Security	Computer Operations and Production Environment Controls

[92] See Adopting Release at p. 154.

[93] See Securities and Exchange Commission Staff Guidance on Current SCI Industry Standards (Nov. 19, 2014), 79 FR 72251. The Staff Guidance can be accessed at: http://www.sec.gov/rules/final/2014/staff-guidance-current-sci-industry-standards.pdf

[94] An SCI Entity's determination not to adhere to some or all of the publications listed in the Staff Guidance in developing its policies and procedures does not necessarily mean that its policies and procedures will be deficient or unreasonable for purposes of Rule 1001(a)(1), *Capacity, integrity, resiliency, availability, and security*. See Adopting Release at p. 193.

[95] See Staff Guidance at p. 5.

The publications are issued by:

- National Institute of Standards and Technology (**NIST**);[96]
- Federal Financial Institutions Examination Council (**FFIEC**);
- Financial Regulator agencies, including the Commission;
- The Institute of Internal Auditors; and
- The Security Benchmarks division of the Center for Internet Security.

Although Commission Staff has stated, in the Staff Guidance, that the above publications are not to be construed as strictly a list of standards, it is their view that these publications satisfy the criteria for current SCI Industry Standards in Rule 1001(a)(4).[97] The publications should be understood to provide guidance to SCI Entities on selecting appropriate controls for applicable systems, as well as suitable processes for developing, documenting, and implementing policies and procedures for their SCI Systems (and Indirect SCI Systems, as applicable), taking into account the criticality of each such system. Thus, it would be reasonable for the most robust controls to be selected and implemented for Critical SCI Systems, as compared to other types of SCI Systems.[98]

Further, the selection of these publications provide guidance to SCI Entities by providing transparency on how Commission Staff will, at least initially, prepare for and conduct inspections relating to Regulation SCI.[99]

Notwithstanding, the Commission believes that it may be appropriate for an SCI Entity to choose to adhere to a standard or guideline in a given domain or subcategory thereof that is different from those contained in the Staff Guidance, and emphasizes that nothing that the Commission Staff may include in its guidance precludes an SCI Entity from adhering to standards such as ISO 27000, COBIT, or other standards, to the extent they result in policies and procedures that comply with the Requirements of Rule 1001(a).[100]

Consistent with the requirements of Rule 1001(a)(4), ISE has developed its Rule 1001(a) policies and procedures incorporating current SCI industry standards. See **Appendix G: Current SCI Industry Standards Mapping**, below, which evidences the publication used for mapping a particular ISE Rule 1001(a) policy.

B. SYSTEMS COMPLIANCE: RULE 1001(b)

Rule 1001(b)(1), *Obligations related to policies and procedures of SCI entities – Systems compliance*, requires that ISE establish, maintain, and enforce written policies and procedures reasonably designed to

[96] Commission Staff notes that NIST, which has published many of the documents contained in the Staff Guidance, is a widely-recognized professional standards organization, and that NIST routinely collaborates with other widely-recognized standards organizations. See Staff Guidance at 5, footnote 9.
[97] See Staff Guidance at 5.
[98] See Adopting Release at p. 193.
[99] See Adopting Release at p. 194.
[100] See Adopting Release at p. 193.

ensure that its SCI Systems operate in a manner that complies with the Act and the rules and regulations thereunder and ISE's rules and governing documents, as applicable.

ISE would not be deemed to be in violation of Rule 1001(b)(1) merely because it experienced a Systems Compliance Issue. Further, the occurrence of a Systems Compliance Issue does not necessarily mean that ISE will be subject to an enforcement action. Rather, the Commission will exercise its discretion to initiate an enforcement action based upon the particular facts and circumstances surrounding the compliance issue.

Rule 1001(b)(2), *Obligations related to policies and procedures of SCI entities – Systems compliance*, requires that ISE establish, maintain, and enforce the following minimum written policies and procedures, reasonably designed to ensure systems compliance:

- Rule 1001(b)(2)(i): Testing of all SCI Systems and any changes to SCI Systems prior to implementation;

- Rule 1001(b)(2)(ii): A system of internal controls over changes to SCI Systems;

- Rule 1001(b)(2)(iii): 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 Act and the rules and regulations thereunder and ISE's rules and governing documents; and

- Rule 1001(b)(2)(iv): 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.

Together, Rules 1001(b)(1) and 1001(b)(2) provide ISE flexibility to establish policies and procedures that are reasonably designed based on the nature, size, technology, business model, and other aspects of its business.[101] These minimum required policies are described below.

1. PRE-IMPLEMENTATION TESTING: RULE 1001(b)(2)(i)

Rule 1001(b)(2)(i), *Obligations related to policies and procedures of SCI entities - Systems compliance*, requires that ISE establish, maintain, and enforce written policies and procedures reasonably designed to ensure that ISE performs testing of all SCI Systems and any changes to SCI Systems prior to implementation.[102] The purpose of this rule is to help ISE identify potential problems before such

[101] See Adopting Release at p. 212.

[102] The Commission understands that SCI SROs generally have procedures to escalate a compliance issue upon discovery, to include legal and compliance personnel in the review of systems changes, and to periodically review rulebooks. See Adopting Release at p. 572. See also, *Rule Change Process Document* referenced in *Internal Controls Over Changes to SCI Systems: Rule 1001(b)(2)(ii)* and *Plan of Communication and Coordination: Rule 1001(b)(2)(iv)*, below.

problems have the ability to impact markets and investors,[103] as well as identify potential compliance issues before new systems or systems changes are implemented.[104]

ISE should consider, on an ongoing basis, the steps it needs to take in order to ensure that these policies and procedures are reasonably designed, including whether they should provide for testing of certain systems changes *after* their implementation to ensure that they operate in compliance with the Exchange Act and relevant rules.[105]

Consistent with the requirements of Rule 1001(b)(2)(i), the *Software Quality Management Procedures Document* governs testing of releases containing new or changed functionality. Additionally, the *ISE Information Security Policy* outlines policy relating to IT Infrastructure Planning, Testing and Acceptance to minimize the risk of system failures, as well as policy on Information Systems and Change Control which requires the introduction of new information systems and major changes to existing information systems to follow a formal process of documentation, specification, testing, quality control, and managed implementation.

2. INTERNAL CONTROLS OVER CHANGES TO SCI SYSTEMS: RULE 1001(b)(2)(ii)

Rule 1001(b)(2)(ii), *Obligations related to policies and procedures of SCI entities – Systems compliance*, requires that ISE establish, maintain, and enforce written policies and procedures reasonably designed to ensure that ISE establishes and maintains a system of internal controls over changes to SCI Systems. The purpose of this rule is to help ISE remain vigilant against compliance issues when changing its systems and resolving potential compliance issues before the changes are implemented.[106]

Although there is no minimum standard for internal controls, a system of internal controls and ongoing monitoring of systems functionality are intended to help prevent SCI Systems from becoming noncompliant resulting from, for example, inattention or failure to review compliance with established written policies and procedures. Internal controls would likely include, for example, protocols that provide for:

- 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; and
- Monitoring of systems changes after implementation.[107]

Consistent with the requirements of Rule 1001(b)(2)(ii), the *ISE Change Management Policy & Process Document* provides a framework for ISE's change management process. Additionally, the *Information*

[103] See Adopting Release at p. 221.
[104] See Adopting Release at p. 652.
[105] See Adopting Release at p. 222.
[106] See Adopting Release at p. 652.
[107] See Adopting Release at p. 223.

Security [ ] Program Plan is an annually updated policy which addresses ISE information security initiatives and related environment controls, and the *Rule Change Process Document* documents the requirement for appropriate communication and coordination between legal, regulatory and business departments when there are changes or other activities impacting SCI Systems. Finally, the *ISE Information Security Policy* outlines policy relating to operations and change management for information processing facilities and information systems.

3. PLAN FOR ASSESSMENTS OF SCI SYSTEM FUNCTIONALITY: RULE 1001(b)(2)(iii)

Rule 1001(b)(2)(iii), *Obligations related to policies and procedures of SCI entities – Systems compliance*, requires that ISE establish, maintain, and enforce written policies and procedures that include 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 Act and the rules and regulations thereunder and ISE's rules and governing documents.

Regulation SCI gives ISE discretion in determining the manner and frequency of assessments because the Commission believes that each SCI Entity will likely be in the best position to assess and determine the assessment plan that is most appropriate for its SCI Systems. 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.[108]

Under Regulation SCI, ISE's plan for assessments could include, for example, not only a plan for monitoring, but also a plan for testing or assessments, as appropriate, and at a frequency (*e.g.*, periodic or continuous) that is based on ISE's risk assessment of each SCI System.[109]

Although the Commission is not requiring SCI Entities to include independent validation in their assessment plans, ISE could determine that its reasonably designed systems compliance policies and procedures should provide for independent validation in its assessment plan under certain circumstances, and design its policies and procedures accordingly. In that case, pursuant to Rule 1001(b), which requires an SCI Entity to establish, maintain, and enforce its written policies and procedures, ISE would be required to enforce its own policies and procedures, including those related to independent validation,[110] if applicable.

Consistent with the requirements of Rule 1001(b)(2)(iii), the *Regulation SCI – Systems Compliance Policy & Procedures* provides ISE's plan for assessments of the functionality of its SCI Systems.

4. PLAN OF COORDINATION AND COMMUNICATION: RULE 1001(b)(2)(iv)

Rule 1001(b)(2)(iv), *Obligations related to policies and procedures of SCI entities – Systems compliance*, requires that ISE establish, maintain, and enforce written policies and procedures that include a plan of coordination and communication between regulatory and other personnel of ISE, including by

[108] See Adopting Release at p. 225-26.
[109] See Adopting Release at p. 225.
[110] See Adopting Release at p. 226.

Responsible SCI Personnel, regarding SCI Systems design, changes, testing, and controls designed to detect and prevent Systems Compliance Issues.

Assessments of SCI Systems compliance by personnel familiar with applicable laws and rules, and regulatory personnel review of SCI Systems design, changes, testing, and controls, are intended to help foster coordination between information technology and regulatory staff so that SCI Events and other issues related to SCI Systems are addressed by a team of ISE Staff in possession of the requisite range of knowledge and skills. They are also intended to help 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.[111]

Consistent with the requirements of Rule 1001(b)(2)(iv), the *Rule Change Process Document* documents the requirement for appropriate communication and coordination between legal, regulatory and business departments when there are changes or other activities impacting SCI Systems.

5. Periodic Review of Effectiveness of Rule 1001(b) Policies: Rule 1001(b)(3)

Rule 1001(b)(3), *Obligations related to policies and procedures of SCI entities – Systems compliance*, requires ISE to periodically review the effectiveness of the policies and procedures required by Rule 1001(b), and take prompt action to remedy deficiencies in such policies and procedures. As detailed above, these policies govern the following activities applicable to ISE's SCI Systems: (i) pre-implementation testing; (ii) internal controls over changes to SCI Systems; (iii) plan for assessments of SCI System functionality; and (iv) plan of coordination and communication.

The Commission has stated that ISE will not be found to be in violation of this maintenance requirement solely because it failed to identify a deficiency immediately after the deficiency occurred, if ISE takes *prompt action* to remedy the deficiency once it is discovered, and ISE had otherwise appropriately reviewed the effectiveness of its policies and procedures and took prompt action to remedy those deficiencies that were discovered.[112]

Consistent with the requirements of Rule 1001(b)(3), ISE shall review and update its Rule 1001(b), *Systems compliance*, policies and procedures **annually**, the timing of which shall be coordinated by management each year. This management review and update is independent of the audit of the effectiveness of such policies and procedures as described in *Audit of the Effectiveness of Rule 1001 Policies and Procedures*, below.

6. Systems Compliance Safe Harbor from liability for Individuals: Rule 1001(b)(4)

Regulation SCI imposes direct obligations on SCI Entities and does not impose obligations directly on personnel of SCI Entities. However, as with all other violations of the Exchange Act and rules that impose

[111] See Adopting Release at p. 227.
[112] See Adopting Release at p. 217.

obligations on an entity, there is a potential for secondary liability for an individual who aided and abetted or caused a violation.[113]

Rule 1001(b)(4), which falls under the *Systems Compliance* umbrella of Regulation SCI, provides a safe harbor from liability, subject to certain conditions, to ISE Staff (**Individual Safe Harbor**). The Individual Safe Harbor applies to "all personnel of an SCI Entity." This includes contractors, consultants, and other non-employees used by ISE in connection with its SCI Systems.[114]

The Individual Safe Harbor only applies to Systems Compliance. ISE is required to comply with the Exchange Act, the rules and regulations thereunder, and its own rules and governing documents, as applicable, and the purpose of Rule 1001(b), *Systems Compliance*, is to effectively help ensure compliance of the operation of SCI Systems with these laws and rules.[115]

The Individual Safe Harbor rule has two prongs: the first applies to all 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.

In particular, Rule 1001(b)(4) states that ISE Staff shall be deemed not to have aided, abetted, counseled, commanded, caused, induced, or procured the violation by ISE of Rule 1001(b) if the ISE Staff member:

- Rule 1001(b)(4)(i): Has reasonably discharged the duties and obligations incumbent upon such person by ISE's policies and procedures; and

- Rule 1001(b)(4)(ii): Was without reasonable cause to believe that ISE's policies and procedures relating to an SCI System for which such ISE Staff 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.[116]

However, the Commission has stated that ISE Staff will not be deemed to have aided, abetted, counseled, commanded, caused, induced, or procured the violation by ISE of Regulation SCI merely because ISE experienced a Systems Compliance Issue, whether or not the ISE Staff member was able to take advantage of the Individual Safe Harbor.[117]

a) Complying With Rule 1001(b)(4): Individual Safe Harbor

In order to be covered by the Individual Safe Harbor, all ISE Staff must reasonably discharge their duties and obligations pursuant to ISE's policies and procedures for systems compliance.

ISE Staff who are responsible for an SCI System, or who have supervisory responsibility concerning SCI Systems, in addition to reasonably discharging their duties, must also be without reasonable cause to

[113] See Adopting Release at p. 232.
[114] See Adopting Release at p. 233.
[115] See Adopting Release at p. 214.
[116] See Adopting Release at p. 233.
[117] See Adopting Release at pp. 235-36.

believe the systems compliance policies and procedures were not established, maintained or enforced in any material respect.

ISE Staff who are not responsible for, *and* do not have supervisory responsibility over, SCI Systems. ISE Staff who are not responsible for, *and* do not have supervisory responsibility over, an SCI System can qualify for the Individual Safe Harbor, *regardless of their belief* regarding the reasonableness of ISE's systems compliance policies and procedures, and are therefore not "deputized to police" the actions of other ISE Staff.[118] These 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** they *discharged their duties and obligations* under the policies and procedures in a *reasonable manner*, in compliance with Rule 1001(b)(4)(i).[119]

ISE Staff who are responsible for, *or* have supervisory responsibility over, SCI Systems. In addition to the first prong of the Individual Safe Harbor, above, which applies to all ISE Staff, this second prong (Rule 1001(b)(4)(ii)) imposes a higher burden on:

- ISE Staff who are responsible for SCI Systems; and
- ISE Staff with supervisory responsibility over others' activities related to an SCI System.

The ISE Staff in these roles likely already have the responsibility to supervise others' activities related to a particular SCI System, and they would already have information to form a reasonable belief regarding the reasonableness of the policies and procedures. When ISE Staff subject to Rule 1001(b)(4)(ii) become aware of potential material noncompliance of ISE's policies and procedures related to an SCI System, such ISE Staff should take action to:

- review and address, or
- direct other personnel to review and address,

such material non-compliance.[120] Therefore, ISE Staff who have responsibility for an SCI System, or who have supervisory responsibility over others' activities related to SCI System(s), are required to be knowledgeable about ISE's systems compliance policies and procedures and should be trained in such systems compliance policies and procedures.

Training of ISE Staff, as described in *Training*, above, is an important component to ensuring that ISE Staff are aware of their duties under Regulation SCI so that they may be able to avail themselves of the Rule 1001(b)(4) Individual Safe Harbor, should the need to do so ever arise.

C. RESPONSIBLE SCI PERSONNEL: RULE 1001(c)

Generally speaking, Regulation SCI requires that ISE notify the Commission of the occurrence of SCI Events[121] and disseminate information to ISE's members regarding these SCI Events.[122] In order to facilitate these obligations, Responsible SCI Personnel, and their designees, play a critical role.

---

[118] See Adopting Release at p. 235.
[119] See Adopting Release at p. 236. Emphasis added.
[120] See Adopting Release at p. 235.
[121] SCI Events are described in *SCI Events*, below.
[122] See *Dissemination of SCI Events: Rule 1002(c)*, below.

Pursuant to Rule 1000, *Definitions*, Responsible SCI Personnel means, for a particular SCI System, Critical SCI System or Indirect SCI System impacted by an SCI Event, such senior manager(s) of ISE having responsibility for such system, and their designees.

Under Regulation SCI, responsibilities of Responsible SCI Personnel also include:

- determining (*i.e.*, "having a reasonable basis to conclude") that an SCI Event has occurred, thereby triggering ISE's Regulation SCI obligations with regards to such SCI Event;[123]
- determining the severity of the SCI Event (*i.e.*, SCI Event, Major SCI Event, or De Minimis SCI Event);
- performing assessments (pursuant to an established plan) of the functionality of SCI Systems designed to detect Systems Compliance Issues, along with other ISE personnel familiar with the Act and the rules and regulations thereunder and ISE's rules and governing documents;[124]
- coordination and communication (pursuant to an established plan) with regulatory and other personnel of ISE regarding SCI Systems design, changes, testing, and controls designed to detect and prevent Systems Compliance Issues;[125] and
- coming to a reasonable estimate of ISE members who may have been affected by the SCI Event for purposes of information dissemination to such members,[126] unless the SCI Event is deemed to be a Major SCI Event, in which instance information dissemination is required for all ISE members.[127]

Rule 1001(c)(1), *Responsible SCI personnel*, requires that ISE establish, maintain, and enforce reasonably designed written policies and procedures that include the criteria for identifying Responsible SCI Personnel, the designation and documentation of Responsible SCI Personnel, and escalation procedures to quickly inform Responsible SCI Personnel of potential SCI Events.

1. CRITERIA FOR IDENTIFYING RESPONSIBLE SCI PERSONNEL: RULE 1001(C)(1)

Consistent with the requirements of Rule 1001(c)(1), *Responsible SCI personnel*, ISE has established the following criteria for identifying Responsible SCI Personnel for each of its SCI Systems, Critical SCI Systems and Indirect SCI Systems.

ISE's criteria for identifying Responsible SCI Personnel for each SCI System[128] and each Indirect SCI System[129] includes (i) the senior manager having responsibility for the SCI system or Indirect System; (ii) a

[123] Rule 1002, *Obligations related to SCI events.*
[124] Rule 1001(b)(2)(iii), *Obligations related to policies and procedures of SCI entities – Systems compliance*. See *Plan for Assessments of SCI System Functionality: Rule 1001(b)(2)(iii)*, above.
[125] Rule 1001(b)(2)(iv), *Obligations related to policies and procedures of SCI entities – Systems compliance*. See *Plan of Coordination and Communication: Rule 1001(b)(2)(iv)*, above.
[126] Information dissemination to members is described in *Dissemination of SCI Events: Rule 1002(c)*, below.
[127] Rule 1002(c)(3), *Obligations related to SCI events. Dissemination of SCI events*.
[128] See **Appendix C: SCI Systems**, for a list of SCI Systems.
[129] See **Appendix E: Indirect SCI Systems**, for a list of Indirect SCI Systems.

level of knowledge and skill to appropriately analyze and assess an issue affecting the SCI System or the Indirect SCI System; and (iii) the authority necessary to take the required actions under Regulation SCI.

Chief Information Officer (CIO). Using the criteria set forth above, ISE has identified its Chief Information Officer (**CIO**) as one of two Responsible SCI Persons for each SCI System with one exception. The one exception is the market surveillance SCI System provided by FINRA, a third party. As further discussed below, the Responsible SCI person for this market surveillance SCI System is the Chief Regulatory Officer (**CRO**). ISE's CIO has responsibility for ISE's information technology and systems, and all issues and decisions affecting its technology. These responsibilities include establishing and implementing technology strategies along with the day to day operations of all of ISE's systems including those identified as SCI Systems. The CIO has considerable knowledge and expertise regarding ISE's large, complex, mission-critical technology environment and their ancillary supporting environments. As an officer of ISE reporting directly to the Chief Executive Officer (**CEO**), the CIO has decision-making authority during critical events and oversees all emergency and disaster recovery/business continuity activities.

Managing Director, ISE Options Exchanges. ISE has also identified the Managing Director of its Options Exchanges as the second Responsible SCI Personnel for each SCI System, except for the market surveillance SCI Systems. The Managing Director oversees the growth and development of the options business and manages its day-to-day operations. The Managing Director is also responsible for the Product Management Group and Market Operations. The Product Management Group is responsible for planning and delivering new trading system functionality to the ISE Options Exchanges. Market Operations is responsible for the day-to-day operations of all ISE Options Exchanges, which includes diagnosing, researching and addressing trading issues. The Managing Director has extensive knowledge and experience regarding the business development and operations of the ISE Options Exchanges, including responsibility for the design of, and changes to, the SCI Systems' functionality. The Managing Director is responsible for coordination and communication between the business development of that functionality and the legal department in order to detect and prevent Systems Compliance Issues at ISE.

Chief Regulatory Officer (CRO). Finally, the Responsible SCI Personnel for the market surveillance SCI Systems are the CIO and the CRO. As indicated above, the CIO has responsibility for all ISE systems including those identified as market surveillance SCI Systems. The CIO's responsibilities for market surveillance are the same as other SCI Systems, except the CIO works with the CRO on the development and functionality of market surveillance systems technology. The CRO is responsible for the oversight of all legal and regulatory functions for the ISE Options Exchanges, including the surveillance programs and the technology used to conduct those programs. The CRO is also responsible for the Regulatory Services Agreement (**RSA**) entered into with FINRA for provision of certain surveillance programs conducted by FINRA on ISE's behalf. In this context, FINRA is considered for purposes of Regulation SCI, a third party provider of an SCI System. Given the interaction the CRO has with FINRA pursuant to the RSA, ISE believes it is appropriate that the CRO be designated the Responsible SCI Personnel for the FINRA-operated market surveillance SCI Systems.

Responsible SCI Personnel for "Indirect SCI Systems." As described in further detail in *Indirect SCI Systems,* above, Indirect SCI Systems are any systems of, or operated by or on behalf of, an SCI Entity that, if breached, would be reasonably likely to pose a security threat to SCI Systems. The Responsible SCI Personnel for an Indirect SCI System will be the same ISE Staff who is the Responsible SCI Personnel for the SCI System that the Indirect SCI System is directly connected to.

2. DESIGNATION AND DOCUMENTATION OF RESPONSIBLE SCI PERSONNEL: RULE 1001(c)(1)

The designation of Responsible SCI Personnel is important so that it is clear who the designated Responsible SCI Personnel are for purposes of the escalation procedures and so that the Commission Staff can easily identify such Responsible SCI Personnel in the course of its inspections, examinations and other interactions with ISE. [130]

Consistent with the requirements of Rule 1001(c)(1), *Responsible SCI personnel*, and the criteria above, ISE has designated a total of three Responsible SCI Personnel for all ISE SCI Systems which are categorized as either trading, order entry/order routing, market data, market regulation, or market surveillance systems.

With certain exceptions, ISE has determined to assign two (2) Responsible SCI Personnel to a particular SCI System, by SCI Event type (*i.e.*, Systems Disruption, Systems Intrusion, and Systems Compliance Issue).[131] The exception applies to market surveillance systems provided by FINRA, a third party. In this instance, ISE's Chief Regulatory Officer is the sole designated Responsible SCI Personnel for the FINRA third party market surveillance system, regardless of SCI Event.

The designated Responsible SCI Personnel, and the SCI Systems for which they are each responsible are provided in **Appendix B: Responsible SCI Personnel – Rule 1001(c)**, below.

a) Designees of Responsible SCI Personnel

The Commission has clarified, in its July 16, 2015 Technology Controls Program (**TCP**) Regulation Systems Compliance and Integrity Outreach Program (**TCP 2015 Reg SCI Outreach**) that designees shall not be used in place of the Responsible SCI Personnel. Designees shall serve only as a backup to the Responsible SCI Personnel in the event the Responsible SCI Personnel is unavailable, due to business travel or vacation, for example. Further, use of a designee does not relieve the Responsible SCI Personnel of his/her obligations under Regulation SCI.

ISE uses the same criteria for identifying designees of Responsible SCI Personnel for each SCI System[132] and each Indirect SCI System[133] as it uses for identifying the Responsible SCI Personnel. Such criteria includes (i) a senior manager having responsibility for the SCI system or Indirect System; (ii) a level of knowledge and skill to appropriately analyze and assess an issue affecting the SCI System or the Indirect SCI System; and (iii) the authority necessary to take the required actions under Regulation SCI.

---

[130] See Adopting Release at p. 244.
[131] See *SCI Events*, below, for further details on SCI Events.
[132] See **Appendix C: SCI Systems**, for a list of SCI Systems.
[133] See **Appendix E: Indirect SCI Systems**, for a list of Indirect SCI Systems.

Refer to **Appendix B-1: Responsible SCI Personnel Designees** for the list of designees.

3. RESPONSIBLE SCI PERSONNEL ESCALATION PROCEDURES: RULE 1001(c)(1)

Rule 1001(c)(1), *Obligations related to policies and procedures of SCI entities – Responsible SCI personnel*, requires (in relevant part) that ISE establish, maintain and enforce reasonably designed written policies and procedures that include escalation procedures to quickly inform Responsible SCI Personnel of potential SCI Events. The purpose of this rule is to require that escalation procedures emphasize *promptness*[134] and to ensure that the appropriate person(s) are provided notice of *potential* SCI Events so that any appropriate actions can be taken in accordance with the requirements of Regulation SCI without unnecessary delay.[135]

The purpose of these **Responsible SCI Personnel Escalation Procedures** is to ensure that Responsible SCI Personnel are quickly informed of incidents affecting SCI Systems in order to allow for meaningful assessment of the incidents and to have a reasonable basis to conclude whether or not the incident is also an SCI Event, prior to triggering any Regulation SCI obligations for ISE. The successful and timely identification of potential SCI Events requires the cooperation and compliance by all ISE Staff, in conjunction with the relevant incident management process as documented in the *ISE Incident Management Policy & Process Document* (Systems Disruptions), *Policy: Information Security Incident Management* (Systems Intrusion) and *Regulation SCI – Systems Compliance Policy & Procedures* (Systems Compliance Issues). Additionally, refer to the *Surveillance Procedures Manual* (*Reg SCI Compliance* Section) for the Market Surveillance Department's discrete incident management process, including Responsible SCI Personnel escalation procedures for all SCI Events (*i.e.*, Systems Intrusions, Systems Disruptions and Systems Compliance Issues) impacting ISE market surveillance systems.

The Commission believes that monitoring in tandem with escalation to Responsible SCI Personnel is an appropriate approach to ensuring SCI compliance.[136] Thus, the reliability of escalation of potential SCI Events to designated Responsible SCI Personnel for determination as to whether they are, in fact, SCI Events is likely to be more effective when it occurs in connection with established procedures for monitoring[137] of SCI Systems and Indirect SCI Systems and pursuant to a process for the communication of systems problems by those who are not Responsible SCI Personnel to those who are.[138]

In order to escalate incidents affecting SCI Systems to ISE Responsible SCI Personnel on a timely basis so that they can determine whether the incident is an SCI Event, the following **Responsible SCI Personnel Escalation Procedures** and related **SCI Event Incident Management Process**, when applicable, will augment, but not replace, ISE's standard overall incident management processes as documented in the *ISE Incident Management Policy & Process Document* (for purposes of escalating Systems Disruptions[139]),

---

[134] See Adopting Release at p. 245.
[135] See Adopting Release at p. 244.
[136] See Adopting Release at p. 180.
[137] See *Systems Monitoring: Rule 1001(a)(2)(vii)*, above.
[138] See Adopting Release at p. 179.
[139] See Rule 1000, *Definitions*.

the *Policy: Information Security Incident Management* (for purposes of escalating Systems Intrusions[140]), the *Regulation SCI – Systems Compliance Policy & Procedures* (for purposes of escalating Systems Compliance Issues), and the *Surveillance Procedures Manual* (*Reg SCI Compliance* Section) (for surveillance incident management policies pertaining to all SCI Event types).

4. RESPONSIBLE SCI PERSONNEL ESCALATION PROCEDURES FOR SYSTEMS DISRUPTIONS (*OTHER THAN MARKET SURVEILLANCE*) – ISE INCIDENT MANAGEMENT

Consistent with Rule 1001(c)(1), *Responsible SCI personnel*, ISE has developed escalation procedures to quickly inform Responsible SCI Personnel of potential SCI Events which may be Systems Disruptions, as described below.

A Note On Market Surveillance: As described in *Responsible SCI Personnel Escalation Procedures – Market Surveillance Department*, below, the Market Surveillance Department has a discrete incident management process for Systems Disruptions which is documented in the *Surveillance Procedures Manual* (*Reg SCI Compliance* Section).

There are three stages to the Responsible SCI Personnel Escalation Procedures which occur contemporaneously with, and are meant to augment and not replace, the incident management process documented in the *ISE Incident Management Policy & Process Document*:

- Incident Detection;
- Incident escalation to Responsible SCI Personnel (only for incidents affecting SCI Systems); and
- Implementing the SCI Event Incident Management Process, if applicable.

a) Incident Detection – Systems Disruptions

Incidents that are potential SCI Events (*i.e.,* Systems Disruptions) can be detected in several ways: via (i) monitoring; (ii) ISE Staff; or (iii) third parties.[141]

Monitoring.[142] Regulation SCI requires that ISE establish, maintain and enforce written policies and procedures that include monitoring of its SCI Systems and, for purposes of security standards, Indirect SCI Systems to identify potential SCI Events.[143] As part of the incident management process documented in the *ISE Incident Management Policy & Process Document*, Application Support, Network Services and

---

[140] See Rule 1000, *Definitions*.
[141] See *ISE Incident Management Policy & Process Document*.
[142] The Commission has stated that escalation of a systems problem should occur not only if a systems problem is identified by chance, but rather, ISE should have a monitoring process in place so that systems problems are identified as a matter of standard operations and pursuant to reasonably established parameters. See Adopting Release at p. 179.
[143] Rule 1001(a)(2)(vii), *Obligations related to policies and procedures of SCI entities – Capacity, integrity, resiliency, availability, and security.*

Market Operations (collectively, the **Level 1 Operational Groups**) employ numerous monitoring tools[144] as the primary means of identifying incidents. These tools are continuously updated and enhanced to improve identification of abnormalities and alerting of the **Level 1 Teams**. The Level 1 Teams are the operational teams that typically are the first to detect an incident, as well as perform initial diagnostics and impact assessment. Other groups within ISE, such as the Surveillance[145] and Facilities departments, utilize their own monitoring and alerting tools and can report an incident occurring within their respective areas.

The Level 1 Teams, as stewards of the incident management process, must immediately determine whether an incident detected by a monitoring tool impacts an SCI System. See **Appendix C: SCI Systems**, below.

ISE Staff. All ISE Staff must be vigilant in their daily routine so that they may detect any systems issue(s) that may occur. These include, but are not limited to: (i) a system failing to work as intended; (ii) a cyber attack, potential criminal activity, or other unauthorized attempt to retrieve, manipulate, or destroy data, or access or disrupt ISE systems;[146] or (iii) any other suspicious activity or malfunction.

All ISE Staff are required to immediately notify the relevant Level 1 Team of any systems issue(s) they encounter in their day-to-day routines and not attempt to self-diagnose the issue. Upon receipt of such notification, the Level 1 Teams must immediately determine whether the incident detected by ISE Staff impacts an ISE system subject to Regulation SCI, as detailed in **Appendix C: SCI Systems**, below.

Third Parties. Third parties may also detect a systems issue affecting ISE. Third parties include: (i) market data vendors, (ii) connectivity providers, (iii) trading customers; or (iv) building management and security.[147]

Upon receipt of such third party alert, the Level 1 Teams must immediately determine whether the incident impacts an SCI System.

b) Incident Escalation to Responsible SCI Personnel – Systems Disruptions

Upon notification of the occurrence of an incident, whether via monitoring tool, ISE Staff, or third party, or by their own discovery, the **Level 1 Teams** must *immediately* determine whether the affected system is an SCI System by referring to **Appendix C: SCI Systems**, below.

If the affected system is *not* an SCI System, the Level 1 Teams will follow the standard ISE Incident Management process documented in the *ISE Incident Management Policy & Process Document*.

---

[144] Refer to the *Application Support/Operations – Tool Inventory List* for the list of monitoring tools utilized.
[145] See *ISE Market Surveillance Reg SCI Compliance Policy and Procedures.*
[146] See Adopting Release at p. 141.
[147] Source: *ISE Incident Management Policy & Process Document.*

If the affected system *is* an SCI System, in addition to the standard ISE Incident Management process, the Level 1 Teams must implement the **Responsible SCI Personnel Escalation Procedures** as follows:

- **Immediately escalate** the occurrence of the incident to the Responsible SCI Personnel for the affected SCI System so that the Responsible SCI Personnel can be made aware of the potential SCI Event and begin to determine whether the incident is an SCI Event and the nature of the SCI Event (*i.e.*, SCI Event, Major SCI Event, or De Minimis SCI Event, as described in *SCI Events*, below).
  - Escalation must occur even if only preliminary information is known at this point.
  - Escalation to the Responsible SCI Personnel can be done via phone or email or in person.

The Level 1 Teams have no discretion with regards to this requirement. ALL incidents impacting an SCI System must be immediately escalated to the appropriate Responsible SCI Personnel. The Responsible SCI Personnel are the only ISE personnel with the regulatory authority to determine whether or not the incident impacting an SCI System is an SCI Event, including the nature of the SCI Event, thereby triggering ISE's Regulation SCI obligations with regards to the incident.

- **Concurrently**, the Level 1 Teams will implement the normal Incident Management process described in the *ISE Incident Management Policy & Process Document*.

- **Implement SCI Event Incident Management Process, if applicable:** To the extent the Responsible SCI Personnel, after performing meaningful assessment of the escalated incident, has/have a reasonable basis to conclude that the incident is an SCI Event (including the nature of the SCI Event), the Responsible SCI Personnel will notify the Level 1 Teams who must then implement the **SCI Event Incident Management Process**, described in *SCI Event Incident Management Process*, below, to occur concurrently with the normal Incident Management Process documented in the *ISE Incident Management Policy & Process Document*.

5. Responsible SCI Personnel Escalation Procedures For Systems Intrusions (*Other Than Market Surveillance*) – ISE Information Security Incident Management

Consistent with Rule 1001(c)(1), *Responsible SCI personnel*, ISE has developed escalation procedures to quickly inform Responsible SCI Personnel of potential SCI Events which may be Systems Intrusions, as described below.

A Note On Market Surveillance: As described in *Responsible SCI Personnel Escalation Procedures – Market Surveillance Department*, below, the Market Surveillance Department has a discrete incident management process for Systems Intrusions which is documented in the *Surveillance Procedures Manual* (*Reg SCI Compliance* Section). Notwithstanding, the ISE market surveillance system falls under the company-wide policies and procedures regarding information security.[148]

[148] See *Surveillance Procedures Manual* (*Reg SCI Compliance* Section).

There are three stages to the Responsible SCI Personnel Escalation Procedures which occur contemporaneously with, and are meant to augment and not replace, the information security incident management process documented in the *Policy: Information Security Incident Management.*

- Incident Detection;
- Incident escalation to Responsible SCI Personnel (only for *successful* intrusions affecting SCI Systems or Indirect SCI Systems); and
- Implementing the SCI Event Incident Management Process, if applicable.

a) Incident Detection – Systems Intrusions

Information security incidents that are potential SCI Events (*i.e.*, Systems Intrusions) can be detected in several ways: via (i) monitoring; and (ii) ISE Staff.

Monitoring.[149] Regulation SCI requires that ISE establish, maintain and enforce written policies and procedures that include monitoring of its SCI Systems and, for purposes of security standards, Indirect SCI Systems to identify potential SCI Events.[150] As stated in the *Policy: Information Security Incident Management,* ISE proactively monitors indicators such as network monitoring or technology watch functions as part of the Preparation Phase of incident response. During the Detection and Analysis Phase of incident response, ISE identifies and correlates the indicators being monitored to determine any notable activity that might suggest malicious behavior or identify risk and threats to the enterprise infrastructure.

The Computer Security Incident Response Team (**CSIRT**), in particular, the Security Analyst, must immediately determine whether an incident detected by a monitoring tool impacts an SCI System or Indirect SCI System. See **Appendix C: SCI Systems**, and **Appendix E: Indirect SCI Systems**, respectively, below.

ISE Staff. All ISE Staff must be vigilant in their daily routine so that they may detect any potential systems issue(s) that may occur. These include, but are not limited to: (i) a system failing to work as intended; (ii) the inadvertent access to a system for which the ISE Staff know they do not, or should not, have access to;[151] (iii) intrusion attempts to introduce malware[152] including, for example, phishing emails containing

[149] The Commission has stated that escalation of a systems problem should occur not only if a systems problem is identified by chance, but rather, ISE should have a monitoring process in place so that systems problems are identified as a matter of standard operations and pursuant to reasonably established parameters. See Adopting Release at p. 179.

[150] Rule 1001(a)(2)(vii), *Obligations related to policies and procedures of SCI events – Capacity, integrity, resiliency, availability, and security.*

[151] The definition of Systems Intrusion is intended to cover unauthorized access, whether intentional or inadvertent, by employees or agents of ISE that resulted from weaknesses in ISE's access controls and/or procedures. See Adopting Release at p. 141.

[152] See Adopting Release at p. 141.

attachments likely to contain malware; (iv) a cyber attack, potential criminal activity, or other unauthorized attempt to retrieve, manipulate, or destroy data, or access or disrupt ISE systems;[153] or (v) any other suspicious activity or malfunction.

All ISE Staff are required to immediately notify the CSIRT of any information security systems issue(s) / systems intrusions they encounter in their day-to-day routines and not attempt to self-diagnose the issue. Upon receipt of such notification, the CSIRT Security Analyst must immediately determine whether the incident detected by ISE Staff impacts an SCI System as detailed in **Appendix C: SCI Systems**, or an Indirect SCI System as detailed in **Appendix E: Indirect SCI Systems**, below.

Note: For details on the primary roles and responsibilities which help establish the foundation of ISE's Information Security Program refer to the *ISE Information Security Program Roles and Responsibilities*.

b) Incident Escalation to Responsible SCI Personnel – Systems Intrusions

Upon notification of the occurrence of an incident that is a successful intrusion, whether via monitoring tool or ISE Staff, or by their own discovery, the **CSIRT'S Security Analyst** must *immediately* determine whether the affected system is an SCI System by referring to **Appendix C: SCI Systems**, or an Indirect SCI System by referring to **Appendix E: Indirect SCI Systems**, below.

If the affected system is *not* an SCI System or Indirect SCI System, the CSIRT will follow the standard Information Security Incident Management process in the *Policy: Information Security Incident Management*.

If the affected system *is* an SCI System or Indirect SCI System, the CSIRT Security Analyst must immediately notify the CSIRT Leader who is an Information Security Director or Department Head. The Information Security Director or Department Head will implement the **Responsible SCI Personnel Escalation Procedures** as follows:

- **Immediately escalate** the occurrence of the successful information security incident to the Responsible SCI Personnel for the affected SCI System or Indirect SCI System, as applicable, so that the Responsible SCI Personnel can be made aware of the potential SCI Event and begin to determine whether the incident is an SCI Event and the nature of the SCI Event (*i.e.*, SCI Event, Major SCI Event, or De Minimis SCI Event, as described in *SCI Events*, below).
    - Escalation must occur even if only preliminary information is known at this point.
    - Escalation to the Responsible SCI Personnel can be done via phone or email or in person.

Neither the CSIRT Security Analyst nor CSIRT Leader have discretion with regards to this requirement. ALL *successful* intrusion incidents impacting an SCI System or Indirect SCI System must be immediately escalated to the appropriate Responsible SCI Personnel. The Responsible SCI Personnel are the only ISE personnel with the regulatory authority to determine whether or not the successful Systems Intrusion

[153] See Adopting Release at p. 141.

impacting an SCI System or Indirect SCI System is an SCI Event, including the nature of the SCI Event, thereby triggering ISE's Regulation SCI obligations with regards to the incident.

- **Concurrently**, the CSIRT will implement the normal Information Security Incident Management process in the *Policy: Information Security Incident Management*.

- **Implement SCI Event Incident Management Process, if applicable:** To the extent the Responsible SCI Personnel, after performing meaningful assessment of the escalated incident, has/have a reasonable basis to conclude that the incident is an SCI Event (including the nature of the SCI Event), the Responsible SCI Personnel will notify the CSIRT Leader who must then implement the **SCI Event Incident Management Process**, as described in *SCI Event Incident Management Process* below, to occur concurrently with the normal Information Security Incident Management Process documented in the *Policy: Information Security Incident Management*.

6. Responsible SCI Personnel Escalation Procedures For Systems Compliance Issues (*Other than Market Surveillance*)

Consistent with Rule 1001(c)(1), *Responsible SCI personnel*, ISE has developed escalation procedures to quickly inform Responsible SCI Personnel of potential SCI Events which may be Systems Compliance Issues, as described below.

A Note On Market Surveillance: As described in *Responsible SCI Personnel Escalation Procedures – Market Surveillance Department*, below, the ISE Market Surveillance Department has a discrete incident management process for Systems Compliance Issues which is documented in the *Surveillance Manual* (*Reg SCI Compliance* Section).

There are three stages to the Responsible SCI Personnel Escalation Procedures which occur contemporaneously with, and are meant to augment and not replace, the systems compliance process documented in the *Regulation SCI – Systems Compliance Policy and Procedures.*

- Incident Detection;

- Incident escalation to Responsible SCI Personnel (only for incidents affecting SCI Systems); and

- Implementing the SCI Event Incident Management Process, if applicable.

a) Incident Detection – Systems Compliance Issues

Systems issues that are potential SCI Events (*i.e.*, System Compliance Issues) can be detected in three ways: (i) monitoring; (ii) ISE Staff; or (iii) externally by a member or other market participant.

Monitoring. Regulation SCI requires that ISE establish, maintain and enforce written policies and procedures that include monitoring of its SCI Systems and, for purposes of security standards, Indirect

SCI Systems to identify potential SCI Events.[154] As stated in the *Regulation SCI – Systems Compliance Policy and Procedures*, ISE has several ways of monitoring for potential Systems Compliance Issues, including through ISE's System Investigation Request Enhanced (**SIRE**) tool which is used to track software issues (referred to as defects and enhancements) in all stages: development, testing, and production. Whenever a defect is detected or an enhancement requested, an ISE Project SIR ("SIR") is created. Each SIR contains specific information about the defect or enhancement including the system involved (e.g. ISE Core (component of T7), Market Data, Trade Manager, etc.), the environment in which the defect occurs or for which the enhancement is requested (e.g. Development, Business Acceptance Testing, Production, etc.), and severity of the issue and its priority to be addressed. Thus, any software defect or error that could be a potential Systems Compliance Issue will be logged into SIRE. A weekly meeting, conducted by SQM, is held to review all SIRs logged the previous week for the ISE Core, while other product managers handle SIRs logged for SCI systems that are not part of the ISE Core. These meetings include representatives of various departments such as the Software Development, Compliance and the Product Management Group.

ISE Staff. There are several stakeholder departments whose Staff may be on the front line of detecting a potential Systems Compliance Issue: (i) Compliance Department; (ii) Legal Department; (iii) Business Development; (iv) Market Operations; (v) Product Management Group; (vi) Software Development; (vii) Software Quality Management; (viii) Technology Support Systems; (ix) Systems Integration Testing; and (x) Market Surveillance Department.

Member or Other Market Participant. ISE may also learn of a potential Systems Compliance Issue from external sources, for example, when a member notifies Market Operations of a system issue affecting that member.

b) Incident Escalation to Responsible SCI Personnel – Systems Compliance Issues

Upon notification of the occurrence of a systems issue, the Product Management Group, with assistance from the Compliance Officer and/or the Legal Department, will review the systems issue and determine whether it is a potential Systems Compliance Issue under Regulation SCI – *i.e.*, whether it impacts an SCI System and whether the issue has caused any SCI System to operate in a manner that does not comply with the Exchange Act and the rules and regulations thereunder or ISE's rules, as applicable..

If, after analysis, the Product Management Group determines that the systems issue is a potential Systems Compliance Issue, the Product Management Group must implement the **Responsible SCI Personnel Escalation Procedures as follows:**

- **Immediately escalate** the potential Systems Compliance Issue to the Responsible SCI Personnel for the affected SCI System so that the Responsible SCI Personnel can be made aware of the potential SCI Event and begin to determine whether the systems issue is an SCI Event and the

[154] Rule 1001(a)(2)(vii), *Obligations related to policies and procedures of SCI events – Capacity, integrity, resiliency, availability, and security.*

nature of the SCI Event (*i.e.*, SCI Event, Major SCI Event, or De Minimis SCI Event, as described in *SCI Events*, below).

- Escalation must occur even if only preliminary information is known at this point.
- Escalation to the Responsible SCI Personnel can be done via phone or email or in person.

The Product Management Group has no discretion with regards to this requirement. ALL systems issues that have been determined to be potential Systems Compliance Issues (*i.e.*, they impact an SCI System) must be immediately escalated to the appropriate Responsible SCI Personnel. The Responsible SCI Personnel are the only ISE personnel with the regulatory authority to determine whether or not the incident impacting an SCI System is an SCI Event, including the nature of the SCI Event, thereby triggering ISE's Regulation SCI obligations with regards to the incident.

- **Concurrently**, the Product Management Group will implement its normal systems issue Incident Management process as described in the **SIRE** section of the *Regulation SCI – Systems Compliance Policy and Procedures*.

- **Implement SCI Event Incident Management Process, if applicable:** To the extent the Responsible SCI Personnel, after performing meaningful assessment of the escalated incident, has/have a reasonable basis to conclude that the incident is an SCI Event (including the nature of the SCI Event), the Responsible SCI Personnel will notify the Product Management Group which must then implement the **SCI Event Incident Management Process**, as described in *SCI Event Incident Management Process* below, to occur concurrently with the normal systems issue Incident Management process as described in the **SIRE** section of the *Regulation SCI – Systems Compliance Policy and Procedures*.

7. Responsible SCI Personnel Escalation Procedures – Market Surveillance Department

ISE's Market Surveillance Department maintains its Regulation SCI compliance procedures in the *Surveillance Procedures Manual* (*Regulation SCI Compliance* Section), including the escalation procedures for Systems Disruption, Systems Intrusions, and Systems Compliance Issues.

- **Systems Disruptions.** All Systems Disruptions will be reported to the ISE Compliance Officer at the same time the Responsible SCI Personnel is notified. The Responsible SCI Personnel will evaluate each Systems Disruption to determine whether it is an SCI Event and the nature of such event (*i.e.*, SCI Event, Major SCI Event, De Minimis SCI Event).

- **Systems Intrusions:** All Systems Intrusions will be reported to the ISE Compliance Officer at the same time the Responsible SCI Personnel is notified. The Responsible SCI Personnel will evaluate

each Systems Intrusion to determine whether it is an SCI Event and the nature of such event (*i.e.*, SCI Event, Major SCI Event, De Minimis SCI Event).[155]

- **Systems Compliance Issue:** All Systems Compliance Issues will be reported to the ISE Compliance Officer at the same time the Responsible SCI Personnel is notified. The Responsible SCI Personnel will evaluate each Systems Compliance Issue to determine whether it is an SCI Event and the nature of such event (*i.e.*, SCI Event, Major SCI Event, De Minimis SCI Event).

See *Surveillance Procedures Manual* (*Regulation SCI Compliance* Section) for details on the Market Surveillance Department's Responsible SCI Personnel Escalation procedures.

8. SCI Event Incident Management Process[156]

Upon notification from the Responsible SCI Personnel that the escalated incident impacting the SCI System(s) constitutes an SCI Event, the relevant incident teams are required to follow this parallel SCI Event Incident Management Process in addition to their standard incident management processes as documented in the following incident management policies:

- *ISE Incident Management Policy & Process Document* (for Systems Disruptions).
- *Policy: Information Security Incident Management* (for Systems Intrusions).
- *Regulation SCI – Systems Compliance Policy & Procedures* (for Systems Compliance Issues).
- *Surveillance Procedures Manual (Reg SCI Compliance* Section*)* (all SCI Event types affecting Market Surveillance).

FIRST, immediately upon the Responsible SCI Personnel notifying the relevant incident management team that the escalated incident has been deemed an SCI Event, notify the ISE Compliance Officer. This can be verbal or written (*e.g.,* email or **ISE Internal SCI Event Reporting Template**). The purpose of this timeframe is to facilitate the immediate Commission notification requirement, described in *Initial Immediate Notification (Oral or Written): Rule 1002(b)(1)*, below.

SECOND, within 24 hours of the Responsible SCI Personnel notifying the relevant incident management team that the escalated incident has been deemed an SCI Event, promptly prepare the **ISE Internal SCI Event Reporting Template** (described below), or similar document (*e.g.*, the post mortem document), with the information known at the time, even if only preliminary, and submit to the Responsible SCI Personnel and the ISE Compliance Officer. The purpose of this timeframe is to facilitate the 24-hour Commission notification requirement, described in *24-Hour Written Notification: Rule 1002(b)(2)*, below.

THIRD, update and submit the **ISE Internal SCI Event Reporting Template**, or similar document (*e.g.*, the post mortem document), to the Responsible SCI Personnel and ISE Compliance Officer on a regular basis,

[155] The *Surveillance Procedures Manual* (*Reg SCI Compliance* Section) underscores that the Surveillance System falls under the company-wide policies and procedures regarding information security.
[156] See *Surveillance Procedures Manual* (*Reg SCI Compliance* Section) for the Market Surveillance Department's SCI Event Management process.

or upon request, to correct any materially incorrect information previously provided, or when new material information is discovered.[157]

FOURTH, submit the final updated **ISE Internal SCI Event Reporting Template**, or similar document (*e.g.*, the post mortem document), to the Responsible SCI Personnel and ISE Compliance Officer when the SCI Event has been resolved and closed.

a) Internal SCI Event Template

Once the Responsible SCI Personnel concludes that an incident affecting an SCI System is an SCI Event, ISE becomes subject to certain Commission notification requirements[158] as well as information dissemination requirements to ISE members.[159] The purpose of the **ISE Internal SCI Event Reporting Template** (or similar document, *e.g.*, the post mortem document) is to centralize the information gathering process, for Regulation SCI purposes, to, among other things: (i) document the SCI Event and its impact; (ii) track the corrective action taken, and resolution of the incident creating the SCI Event; (iii) facilitate the completion and filing of Form SCI with the Commission, as well as the member dissemination requirement; and (iv) comply with recordkeeping requirements.

The use of the **ISE Internal SCI Event Reporting Template** is optional. Its purpose is to provide ease of reporting the required information to the Responsible SCI Personnel and ISE Compliance Officer. So long as the required information is properly and timely reported, the incident management teams may utilize a similar document for these purposes.

The **SCI Event Incident Management Process** augments ISE's various incident management processes by requiring the relevant incident management team to assign a person to complete an **ISE Internal SCI Event Reporting Template**, or similar document (*e.g.*, the post mortem document), for the particular SCI Event and submit it to the Responsible SCI Personnel and the ISE Compliance Officer, as noted above. The Regulation SCI information to be included in the **ISE Internal SCI Event Reporting Template**, or similar document (*e.g.*, the post mortem document), to facilitate ISE's reporting obligation to the Commission is as follows:

- Rule 1002(b)(2)(i).[160] A description of the SCI Event, including the SCI system(s) affected.

- Rule 1002(b)(2)(ii).[161] To the extent available[162] as of the time of the notification:

[157] Rule 1002(b)(3), *Obligations related to SCI events – Commission notification and recordkeeping of SCI events*.
[158] Rule 1002(b), *Obligations related to SCI events – Commission notification and recordkeeping of SCI events*.
[159] Rule 1002(c), *Obligations related to SCI events – Dissemination of SCI events*.
[160] *Obligations Related to SCI Events – Commission notification and recordkeeping of SCI events*.
[161] *Obligations Related to SCI Events – Commission notification and recordkeeping of SCI events*.
[162] Some of the information required here may not be immediately available, or may only be preliminary. If preliminary information is available, that should be included and indicated as such.

- ISE's (current) assessment of the types and number of market participants (potentially) affected by the SCI Event;[163]
- the (potential) impact of the SCI Event on the market;[164]
- a description of the steps ISE has taken, is taking, or plans to take, with respect to the SCI Event;
- the time the SCI Event was resolved or timeframe within which the SCI Event is expected to be resolved; and
- any other pertinent information known by ISE about the SCI Event.

➢ Rule 1002(b)(3).[165] Until such time as the SCI Event is resolved and ISE's investigation of the SCI Event is closed, provide updates pertaining to such SCI Event to the Responsible SCI Personnel and the ISE Compliance Officer on a regular basis, or at such frequency as requested, to correct any materially incorrect information previously provided, or when new material information is discovered, including but not limited to, any of the information listed in Rule 1002(b)(2)(ii), above.

The **ISE Internal SCI Event Reporting Template** is stored in the **Compliance Department Shared Drive** in the "Templates" sub-folder. It is also available to ISE Staff on the **J Drive** in the **Regulation SCI** folder / "**Toolkit**" sub-folder**.**

A Note Regarding De Minimis SCI Events. Consistent with the requirements of Rule 1002(b)(5), *Obligations related to SCI events – Commission notification and recordkeeping of SCI events*, described in *Commission Notification and Recordkeeping of De Minimis SCI Events: Rule 1002(b)(5)*, below, the incident management teams shall maintain records concerning all SCI Events deemed to be de minimis by the Responsible SCI Personnel. Within **15** calendar days after the end of each calendar quarter, the incident management team must submit a summary description of any such De Minimis SCI Events, including affected SCI Systems and/or Indirect SCI Systems, which occurred during such calendar quarter to the Responsible SCI Personnel and the ISE Compliance Officer. The 15-day internal submission deadline is necessary to facilitate any internal follow up, as well as preparation of the quarterly report on De Minimis SCI Events which is due to the Commission within **30** calendar days after the end of the calendar quarter.

9. Periodic Review of Effectiveness Rule 1001(c) Policies: Rule 1001(c)(2)

Rule 1001(c)(2), *Obligations related to policies and procedures of SCI entities – Responsible SCI personnel*, requires ISE to periodically review the effectiveness of policies and procedures required by Rule 1001(c)(1), and take prompt action to remedy deficiencies in such policies and procedures. As detailed above, these policies govern the following activities applicable to ISE Responsible SCI Personnel: (i) criteria

[163] In the initial preparation of the form, the assessment of impact to members would only be preliminary and based on what is currently known. At the closure of the incident, the impact to market participants must be updated to reflect actual impact resulting from the SCI Event.
[164] In the initial preparation of the form, the impact would only be potential based on what is currently known. At the closure of the incident, the impact to the market must be updated to reflect actual impact resulting from the SCI Event.
[165] *Obligations Related to SCI Events – Commission notification and recordkeeping of SCI events*.

for identifying Responsible SCI Personnel; (ii) designation and documentation of Responsible SCI Personnel; and (iii) Responsible SCI Personnel escalation procedures.

Consistent with the requirements of Rule 1001(c)(2), ISE shall review and update its Rule 1001(c)(1) policies and procedures **annually**, the timing of which shall be coordinated by management each year. This management review and update is independent of the audit of the effectiveness of such policies and procedures as described in *Audit of the Effectiveness of Rule 1001 Policies and Procedures*, below.

INTENTIONALLY LEFT BLANK

VI. SCI EVENTS

As described below, Regulation SCI distinguishes between three categories of events impacting SCI Systems: SCI Event, Major SCI Event and De Minimis SCI Event.

A. SCI EVENT

An **SCI Event** is an event at ISE that constitutes: (1) a Systems Disruption; (2) a Systems Compliance Issue; or (3) a Systems Intrusion.[166] An SCI Event is resolved when the event no longer meets the definition of a Systems Disruption, Systems Intrusion, or Systems Compliance Issue, as defined in Rule 1000.[167] Each of type of SCI Event is described below.

1. SYSTEMS DISRUPTION

A **Systems Disruption** is an event in ISE's SCI Systems that disrupts, or significantly degrades, the normal operation of an SCI System.[168] The definition of Systems Disruption does not limit such events with respect to the *source* of the disruption, *i.e.*, whether an internal source at ISE or an external third party source.[169] Further, some Systems Disruptions may initially seem insignificant, but may later prove to be the cause of significant Systems Disruptions at ISE.[170]

Refer to *Responsible SCI Personnel Escalation Procedures for Systems Disruptions (Other Than Market Surveillance) – ISE Incident Management*, above, for details on ISE's overall incident management process for Systems Disruptions, including its related Responsible SCI Personnel escalation procedures. See also *Surveillance Procedures Manual* (*Reg SCI Compliance* Section) for the Market Surveillance Department procedures for Systems Disruptions. Refer to *SCI Event Incident Management Process*, above, for the Regulation SCI-specific incident management process for SCI Events.

a) Normal Operation of SCI Systems – Regulation SCI Guidance

In determining whether a Systems Disruption has occurred, the Commission states that SCI Entities would likely find it helpful to establish parameters that can aid them and their staff in determining what constitutes the "normal operation" of each of its SCI Systems, and when such "normal operation" has been disrupted or significantly degraded because those parameters have been exceeded.[171]

---

[166] Rule 1000, *Definitions*.
[167] See Adopting Release at p. 297.
[168] Rule 1000, *Definitions*.
[169] See Adopting Release at p. 131.
[170] See Adopting Release at p. 130.
[171] See Adopting Release at p. 126.

In this regard, it would be appropriate for ISE to take into account **regularly scheduled outages** or **scheduled maintenance** as part of "normal operations."[172] A **planned disruption** to an SCI System that is a part of regularly scheduled outages or scheduled maintenance would not constitute a Systems Disruption or be subject to the requirements of Regulation SCI, if such regularly scheduled outages or scheduled maintenance are part of ISE's normal operations.[173]

With regard to **data queuing**, to the extent that such queuing is part of the normal functionality of a system and does not cause a disruption or significant degradation of normal operations, it would not be captured by the rule, which is limited to events occurring to an SCI System that are outside its normal operations.[174]

However, if **loss of […] transaction data** disrupts or significantly degrades the normal operation of an SCI System, it would constitute a Systems Disruption and be subject to the requirements of Regulation SCI (*e.g.*, immediate or quarterly Commission notification, depending upon the impact of the disruption).[175]

Example: If an SCI System experiences an **unplanned outage** but fails over smoothly to its backup system such that there is no disruption or significant degradation of the normal operation of the system, the outage of the primary system would not constitute a Systems Disruption. On the other hand, ISE may determine that, even when a primary system fails over smoothly to its backup system such that users are not impacted by the failover, operating from the backup system without additional redundancy would not constitute normal operation. In this case, the outage of the primary system would fall within the definition of Systems Disruption.[176] The Commission further clarified, in the Regulation SCI FAQs, that, whether the failure of a system component with a seamless failover to a backup system constitutes a Systems Disruption depends on the particular facts and circumstances of the incident. It is not automatically a Systems Disruption simply because a component failed; nor is it automatically excluded from being an SCI Event simply because there was seamless failover. Rather, ISE would have to determine whether such a failure meets the definition of "Systems Disruption" under Rule 1000, *Definitions*.[177]

b) Scope of Normal Operations of ISE SCI Systems

Consistent with the requirements of Regulation SCI, ISE has developed the following time-based parameters to define the baseline scope of normal operations of ISE SCI Systems for purposes of identifying SCI Events that are Systems Disruptions.

Baseline Scope of Normal Operations Defined. As a general rule, for purposes identifying a Systems Disruption (only), ISE considers the normal operations of its SCI Systems to occur between 6:00am Eastern Standard Time (**EST**) and 5:15pm EST.

---

[172] See Adopting Release at p. 128.
[173] See Adopting Release at p. 128.
[174] See Adopting Release at p. 128.
[175] See Adopting Release at p. 129.
[176] See Adopting Release at p. 127.
[177] See Regulation SCI FAQs at: http://www.sec.gov/divisions/marketreg/regulation-sci-faq.shtml

Therefore, the occurrence of an SCI Event that is a Systems Disruption that disrupts, or significantly degrades, the normal operation of an SCI System is dependent upon the time the event occurred and/or corrective action was completed, as described below:

- Events meeting the definition of a Systems Disruption that occur **or** remain unresolved between 6:00am EST and 5:15pm EST are **within the baseline scope of normal operations**, and would be considered Systems Disruptions.

- Events meeting the definition of a Systems Disruption that occur **and** are resolved between 5:16pm EST and 5:59am EST the following morning,[178] are ***not* within the baseline scope of normal operations** and therefore would not be considered a Systems Disruption by ISE.

- Events meeting the definition of a Systems Disruption that occur between 5:16pm EST and 5:59am EST the following morning which are **not resolved** before 6:00am EST[179] will be **within the baseline scope of normal operations** and considered Systems Disruptions.

It is important to note that the baseline time-based scope of normal operations applies to Systems Disruptions only. Events meeting the definition of Systems Compliance Issue or Systems Intrusion are not subject to these time-based parameters, as described below in *Scope of Systems Compliance Issues*, and *Scope of Systems Intrusions*, respectively.

A Note on Market Surveillance. The ISE Market Surveillance Department maintains its own defined "normal operations" for surveillance systems. See *Surveillance Procedures Manual* (*Reg SCI Compliance* Section).

Refer to *Responsible SCI Personnel Escalation Procedures for Systems Disruptions (Other Than Market Surveillance)*, above, for details on ISE's overall incident management process for Systems Disruptions, including its related Responsible SCI Personnel escalation procedures. See also *Surveillance Procedures Manual* (*Reg SCI Compliance* Section) for the Market Surveillance Department procedures for Systems Disruptions. Refer to *SCI Event Incident Management Process*, above, for the Regulation SCI-specific incident management process for SCI Events.

[178] *i.e.*, they are resolved during the period of time deemed to be outside of the time-based scope of normal operations for SCI Systems.
[179] *i.e.*, they are resolved after 6:00am EST and during the time when the SCI System is considered to be within the defined scope of normal operations.

2. SYSTEMS COMPLIANCE ISSUE

A **Systems Compliance Issue** means an event at ISE that has caused any SCI System of ISE to operate in a manner that does not comply with the Act and the rules and regulations thereunder or ISE's rules or governing documents, as applicable.[180]

A Systems Compliance Issue could, for example, occur when a change to an SCI System is made by information technology staff, without the knowledge or input of regulatory staff, which results in the system operating in a manner that does not comply with the Act and rules thereunder or ISE's rules and other governing documents.[181]

Commission Staff has provided guidance[182] on when a Systems Compliance Issue at an SCI SRO (*i.e.*, ISE) would be considered "resolved" under Regulation SCI. This can occur in one of two ways:

- First, the issue could be resolved when the SCI System's functionality is modified so that it operates in accordance with the Act, rules and regulations thereunder, and ISE's existing rules.

- Second, in the case where ISE's systems are operating in a manner that does not comply with ISE's rules or governing documents, but are not otherwise in violation of the Act or rules thereunder, the System Compliance Issue could be resolved by modifying ISE's rules or governing documents to accurately reflect the operation of the system. This would be accomplished by filing a proposed rule change with the Commission under Section 19(b) and the proposed rule change becoming effective or being approved by the Commission, as applicable.

Refer to *Responsible SCI Personnel Escalation Procedures for Systems Compliance Issues (Other Than Market Surveillance)*, above, for details on ISE's overall incident management process for Systems Compliance Issues, including its related Responsible SCI Personnel escalation procedures. See also *Surveillance Procedures Manual* (*Reg SCI Compliance* Section) for the Market Surveillance Department procedures for Systems Compliance Issues. Refer to *SCI Event Incident Management Process*, above, for the Regulation SCI-specific incident management process for SCI Events.

a) Scope of Systems Compliance Issues

Events meeting the definition of a Systems Compliance Issue are within scope 24 hours, daily.

[180] Rule 1000, *Definitions*.
[181] See Adopting Release at p. 137.
[182] See Regulation SCI FAQs at: http://www.sec.gov/divisions/marketreg/regulation-sci-faq.shtml

3. SYSTEMS INTRUSION

Pursuant to Rule 1000, *Definitions*, **Systems Intrusion** means any unauthorized entry into the SCI Systems or Indirect SCI Systems of ISE.[183]

This definition is intended to cover:

- any unauthorized entry into SCI Systems or Indirect SCI Systems, regardless of the identity of the person committing the intrusion (whether they are outsiders, employees, or agents of ISE), and regardless of whether or not the intrusion was part of a cyber-attack, potential criminal activity or other unauthorized attempt to retrieve, manipulate, or destroy data, or access or disrupt systems of ISE.[184]

- the introduction of malware or other attempts to disrupt ISE's SCI Systems or Indirect SCI Systems, provided that such systems were *actually* breached;[185] and

- unauthorized access, whether intentional or inadvertent, by employees or agents of ISE that resulted from weaknesses in ISE's access controls and/or procedures.[186]

The definition of Systems Intrusion does not include unsuccessful attempts at unauthorized entry. Unauthorized entries must be "successful" because the term "entry" incorporates the concept of successfully gaining access to an SCI System or Indirect SCI System.[187]

Refer to *Responsible SCI Personnel Escalation Procedures for Systems Intrusions (Other Than Market Surveillance) – ISE Information Security Incident Management*, above, for details on ISE's overall incident management process for Systems Intrusions, including its related Responsible SCI Personnel escalation procedures. See also *Surveillance Procedures Manual* (*Reg SCI Compliance* Section) for the Market Surveillance Department procedures for Systems Intrusions. Refer to *SCI Event Incident Management Process*, above, for the Regulation SCI-specific incident management process.

A Note on Access Control. The *ISE Information Security Policy* documents ISE's Access Control[188] policies and procedures. The Access Control policies and procedures generally cover the following:

- User, Vendor and Default IDs;
- User Access Management;
- User Authentication and Requirements for External Parties;
- Password Management System;

---

[183] Rule 1000, *Definitions*.
[184] See Adopting Release at p. 140.
[185] See Adopting Release at p. 141.
[186] See Adopting Release at p. 141.
[187] See Adopting Release at p. 141.
[188] As documented in the *ISE Information Security Policy*, access control refers to the process by which restrictions may be placed on users, systems and resources and what specifically may be done with that access.

- Unattended User Equipment;
- Business Application Systems Access Control;
- IT Infrastructure Access Control;
- IT Infrastructure Services;
- IT Infrastructure Remote Access;
- Operating System Access Control; and
- Information and Application Access Control.

a) Scope of Systems Intrusions

Events meeting the definition of a Systems Intrusion are within scope 24 hours, daily. Further, there is no materiality threshold for events meeting the definition of Systems Intrusions.[189]

B. MAJOR SCI EVENT

Rule 1000, *Definitions*, defines a **Major SCI Event** as an SCI Event that has had, or ISE reasonably estimates would have:

- any impact on a Critical SCI System; or

- a significant impact on ISE's operations or on market participants.

A Note on "Significant Impact on Market Participants." The Commission Staff has provided guidance that, rather than focusing solely on the number of market participants impacted, ISE should analyze the facts and circumstances regarding the impact of an SCI Event and may consider how the event affects one or more, or a given group or class, of market participants as a whole and whether it has a "significant impact" on such market participants. In conducting such an analysis, it would be appropriate for ISE to take into account the relative significance of the market participant(s) impacted, whether by trading volume, importance to ISE'S operations, or such other factors ISE determines to be appropriate. For example, if a Systems Disruption only impacts two market makers but such market makers are two of the largest market makers at ISE, such an event *could* constitute a Major SCI Event if the impact on those two participants would be considered significant.[190]

Consistent with the requirements of Regulation SCI, ISE has developed general guidelines for determining whether an event is a Major SCI Event.

[189] See Adopting Release at p. 141.
[190] See Regulation SCI FAQs at: http://www.sec.gov/divisions/marketreg/regulation-sci-faq.shtml

1. Determining Whether an Event is a Major SCI Event – Guidelines Only

The determination of whether an SCI Event rises to the level of a Major SCI Event shall be determined by the Responsible SCI Personnel based on the particular facts and circumstances of each SCI Event. Refer to *Responsible SCI Personnel: Rule 1001(c)*, above, for ISE policies and procedures governing for Responsible SCI Personnel.

C. De Minimis SCI Event

De Minimis SCI Events are SCI Events that have had, or ISE reasonably estimates would have, no or a de minimis impact on ISE's operations or on market participants.[191]

Consistent with the requirements of Regulation SCI, ISE has developed general guidelines for determining whether an SCI Event is a De Minimis SCI Event.

1. Determining Whether an Event is a De Minimis SCI Event – Guidelines Only

The determination of whether an SCI Event is a De Minimis SCI Event will be determined by the Responsible SCI Personnel based on the particular facts and circumstances of each SCI Event. Refer to *Responsible SCI Personnel*: *Rule 1001(c)*, above, for ISE policies and procedures governing for Responsible SCI Personnel.

INTENTIONALLY LEFT BLANK

[191] See Rule 1002(b)(5), *Obligations Related to SCI events – Commission notification and recordkeeping of SCI events*.

VII. REGULATORY OBLIGATIONS RELATED TO SCI EVENTS

Once Responsible SCI Personnel have a reasonable basis to conclude that an SCI Event has occurred, Rule 1002, *Obligations related to SCI events*, requires that ISE satisfy certain regulatory obligations including, taking appropriate corrective action, notifying the Commission of the SCI Event, disseminating information regarding certain SCI Events, and maintaining records relating to all SCI Events, as detailed below.

Development and Testing Systems. Because development and testing systems are not part of the definition of "SCI Systems," systems issues with regard to development and testing systems would not be subject to the requirements of Rule 1002 relating to corrective action, Commission notification, and dissemination of information on SCI Events.[192]

A. CORRECTIVE ACTION: RULE 1002(a)

Pursuant to Rule 1002(a), *Corrective action*, upon any Responsible SCI Personnel having a reasonable basis to conclude that an SCI Event has occurred, ISE shall begin to take appropriate corrective action which shall include, at a minimum:

- mitigating potential harm to investors and market integrity resulting from the SCI Event and
- devoting adequate resources to remedy the SCI Event as soon as reasonably practicable.

Rule 1002(a) permits ISE to perform an initial analysis and preliminary investigation into a potential systems issue before the corrective obligations are triggered. Because the facts and circumstances of each specific SCI Event will be different, this standard would help ensure that ISE takes necessary corrective action soon after an SCI Event, but not without sufficient time to first consider what is the appropriate action to remedy the SCI Event in a particular situation and how such corrective action should be implemented.[193]

Thus, only when: (i) suspected systems problems are escalated to Responsible SCI Personnel and their designees, and (ii) such personnel have a reasonable basis to conclude that an SCI Event has occurred, are the appropriate corrective actions required by Rule 1002(a) triggered.[194] It would not be appropriate for ISE to unnecessarily delay the start of corrective action once the relevant Responsible SCI Personnel have a reasonable basis to conclude that an SCI Event has occurred. [195]

Notwithstanding the above, under ISE's incident management processes, corrective action for all incidents occur as soon as practicable and is not dependent upon, or delayed by, the determination by the Responsible SCI Personnel that the incident is also an SCI Event.

---

[192] See Adopting Release at pp. 158-59, FN 487.
[193] See Adopting Release at p. 658.
[194] See Adopting Release at p. 251.
[195] See Adopting Release at p. 656.

Corrective action would likely include a variety of actions, including:[196]

- determining the scope of the SCI Event and its causes;
- making a determination regarding its known and anticipated impact;
- following adequate internal diagnosis and resolution policies and procedures; and
- taking additional action to respond as ISE deems appropriate.

Documentation and Review of Corrective Action Process. The Commission believes that SCI Entities are likely to work to develop a written process for ensuring that they are prepared to comply with the corrective action requirement and are also likely to periodically review this process.[197] To this end, ISE's respective corrective action processes are integrated into the following incident management-related policies:

- *ISE Incident Management Policy & Process Document*,
- *ISE Incident and Crisis Escalation Process*,
- *Addendum to ISE Incident and Crisis Escalation Process*
- *ISE Problem Management Policy & Process Document*
- *Policy: Information Security Incident Management,*
- *Regulation SCI – Systems Compliance Policy & Procedures*, and
- *Surveillance Procedures Manual* (*Reg SCI Compliance* Section).

Further, as part of its annual SCI Review, ISE's Internal Audit Department (**ISE Internal Audit**) will test the controls for Rule 1002(a), *Obligations related to SCI events – Corrective action*, as documented in the *Regulation SCI: Annual Review Program – Internal Audit Approach.*[198]

A Note On Corrective Action by Third Parties Operating SCI Systems on Behalf of ISE.

- **FINRA:** As documented in FINRA's *Framework for Managing SCI Workflow under RSAs* term sheet, FINRA will take corrective action in accordance with Regulation SCI for all SCI Events impacting systems operated by FINRA on behalf of ISE (*i.e.*, RSA systems). For further detail on the corrected action process, refer to the *Framework for Managing SCI Workflow under RSAs* term sheet, stored on the Compliance Department's shared drive.

- **EXEGY:** As documented in the Exegy *SCI Events Corrective Actions Policy*, Exegy will follow standard operating procedures to take corrective actions for events impacting SCI Systems and will adhere to the Exegy SLA in taking corrective actions for all events impacting SCI Systems. The Exegy *SCI Events Corrective Actions Policy* is stored on the Compliance Department's shared drive.

[196] See Adopting Release at p. 252.
[197] See Adopting Release at p. 458.
[198] ISE Internal Audit Approach 2015.

B. COMMISSION NOTIFICATION AND RECORDKEEPING OF SCI EVENTS: RULE 1002(b)

Under Rule 1002(b), *Commission notification and recordkeeping of SCI events*, SCI Events that ISE reasonably estimates to have a greater than de minimis impact on ISE's operations or on market participants are subject to immediate Commission notification and follow-up reporting until resolved (Rules 1002(b)(1) – (b)(4)). While all De Minimis SCI Events are subject to recordkeeping requirements, de minimis Systems Intrusions and de minimis Systems Disruptions are also subject to quarterly reporting to the Commission (Rule 1002(b)(5)). Thus, de minimis Systems Compliance Issues are only subject to recordkeeping requirements.

A Note On Commission Notification of SCI Events Affecting Third Party SCI Systems Operated on Behalf of ISE.

- **FINRA:** As documented in FINRA's *Framework for Managing SCI Workflow under RSAs* term sheet (**RSA**), FINRA has outlined a process for Commission notification which involves FINRA making immediate notification (generally by email, copying ISE), subject to ISE's agreement and, for subsequent written notifications, providing a draft copy to ISE for review prior to filing with the Commission. Additionally, with regard to recordkeeping, FINRA will share its procedures with ISE for review and provide an annual attestation concerning its compliance with Regulation SCI's recordkeeping requirements. ISE has determined that ISE will designate FINRA personnel as Responsible SCI Personnel for the limited purpose of providing immediate notifications pursuant to Rule 1002(b)(1) to the Commission (by email, copying ISE) as documented in the RSA, but ONLY for Systems Disruptions and Systems Intrusions impacting a FINRA Regulation SCI System operated by FINRA on behalf of ISE. For Systems Compliance Issues affecting a FINRA Regulation SCI System operated by FINRA on behalf of ISE, FINRA must immediately notify ISE and ISE will then notify the Commission. ISE will request confidential protection under the Freedom of Information Act (**FOIA**) or use Form SCI[199] for any notifications made for Systems Compliance Issues affecting a FINRA Regulation SCI System operated by FINRA on behalf of ISE.[200] For further detail on the corrective action process, refer to the *Framework for Managing SCI Workflow under RSAs* term sheet, stored on the Compliance Department's shared drive.

- **EXEGY:** The ISE *Policy: Third Party Providers of SCI Systems – Exegy*, provided to Exegy, outlines notification and recordkeeping requirements for Exegy to comply with. This includes preparing and emailing to ISE (at: ISERegSCIEvents@ise.com) an **ISE SCI Event Notification Form** containing Regulation SCI-required information to facilitate ISE's Commission notification and recordkeeping activities. For details, refer to the *Policy: Third Party Providers of SCI Systems – Exegy*, stored on the Compliance Department's shared drive.

[199] All documents submitted with Form SCI receive FOIA protection.
[200] This was communicated via email to FINRA by the ISE Compliance Officer on October 26, 2015.

1. INITIAL IMMEDIATE NOTIFICATION (ORAL OR WRITTEN): RULE 1002(b)(1)

Pursuant to Rule 1002(b)(1), *Commission notification and recordkeeping of SCI events*, ISE shall, upon any Responsible SCI Personnel having a reasonable basis to conclude that an SCI Event has occurred, notify the Commission of such SCI Event immediately. The initial immediate notification may be given orally (via telephone, at the designated phone number listed below) or in written form (via email at the designated email listed below, or Form SCI, at ISE's discretion[201]).[202]

The requirement for ISE to immediately notify the Commission of a (non-de minimis) SCI Event[203] upon any Responsible SCI Personnel having a reasonable basis to conclude that a (non-de minimis) SCI Event has occurred does not provide a notification exception for periods outside of normal business hours.[204]

Form SCI.[205] Form SCI permits, but does not require, ISE to utilize the form to submit initial notifications of SCI Events pursuant to Rule 1002(b)(1), as well as updates regarding SCI Events pursuant to Rule 1002(b)(3).[206] Although it is not required, Commission Staff encourages SCI Entities to make use of Form SCI in providing the initial immediate notification, when appropriate, as it provides a standardized means for submitting such notifications to the Commission.[207] If ISE chooses to utilize Form SCI to submit an initial notification required by Rule 1002(b)(1), ISE will be able to submit a short description of the SCI Event, and be allowed to attach documents regarding such SCI Event as part of Exhibit 6, *Optional Attachments*, to Form SCI.[208] The use of Form SCI also permits ISE to electronically request confidential treatment of all information filed on Form SCI.[209]

Subject to the relevant Responsible SCI Personnel escalation procedures described in *Responsible SCI Personnel*: *Rule 1001(c)*, and related SCI Event incident management procedures described in *SCI Event Incident Management Process*, above, and pursuant to Rule 1002(b)(1), the ISE Compliance Officer or General Counsel will immediately notify the Commission of the occurrence of the SCI Event, as required by Rule 1002(b)(1).

Notification	Commission Contact
Oral/Telephone	**202 551-6300**.
Email	**cyberwatch@sec.gov**

[201] Rule 1006, *Electronic filing and submission*, provides that immediate Commission notification of (non-de minimis) SCI Events (Rule 1002(b)(1)) and updates regarding SCI Events (Rule 1002(b)(3)) are not required to be filed on Form SCI. See Adopting Release at p. 405.
[202] See Adopting Release at p. 280.
[203] Rule 1002(b)(5), *Obligations related to SCI events – Commission notification and recordkeeping of SCI events*, provides an exception to the immediate notification requirement for de minimis SCI Events, as described in *Commission Notification and Recordkeeping of De Minimis SCI Events: Rule 1002(b)(5)*, below.
[204] See Adopting Release at pp. 280-81.
[205] See *Electronic Filing and Submission (Form SCI): Rule 1006*, below.
[206] See Adopting Release at p. 416.
[207] See Regulation SCI FAQs at: http://www.sec.gov/divisions/marketreg/regulation-sci-faq.shtml
[208] See Adopting Release at p. 423.
[209] See Regulation SCI FAQs.

As advised by Commission Staff during an October 27, 2015 conference call between ISE and the Commission's Cyber Watch Team (the **Cyber Watch Call**), a team of analysts are available to answer the phone **30 minutes prior to market open** and **30 minutes after market close**. During other times, ISE can leave a voicemail for any oral notification.

Confidential Treatment Requests. For any emailed notifications, ISE must make a confidential treatment request in paper format only,[210] pursuant to Rule 24b-2 under the Exchange Act.[211]

Secondary (additional) Notification. The Commission has indicated, in the Regulation SCI FAQs, that, as a secondary notification, ISE **may** *additionally* notify any other Commission Staff it feels appropriate, including any Commission Staff member with whom ISE's personnel consults regarding the issues relating to a given SCI Event.

2. 24-HOUR WRITTEN NOTIFICATION: RULE 1002(b)(2)

Pursuant to Rule 1002(b)(2), *Obligations related to SCI events – Commission notification and recordkeeping of SCI events*, ISE shall, within 24 hours of any Responsible SCI Personnel having a reasonable basis to conclude that an SCI Event has occurred, submit a written notification pertaining to such SCI Event to the Commission, which shall be made on a good faith, best efforts basis and include:

- Rule 1002(b)(2)(i): A description of the SCI Event, including the system(s) affected; and

- Rule 1002(b)(2)(ii): To the extent available as of the time of the notification:
  - ISE's current assessment of the types and number of market participants potentially affected by the SCI Event;
  - the potential impact of the SCI Event on the market;
  - a description of the steps ISE has taken, is taking, or plans to take, with respect to the SCI Event;
  - the time the SCI Event was resolved or timeframe within which the SCI Event is expected to be resolved; and
  - any other pertinent information known by ISE about the SCI Event.

Form SCI. The Rule 1002(b)(2) 24-hour written notification is required to be submitted via Form SCI. In addition to providing the applicable standardized information on Form SCI, as described above, ISE is required to submit an Exhibit 1, *Rule 1002(b)(2) Notification of SCI Event*,[212] which must contain the information required in Rules 1002(b)(2)(i) and 1002(b)(2)(ii), described above. The Exhibit 1, *Rule 1002(b)(2) Notification of SCI Event* Template is stored in the **Compliance Department Shared Drive** in the "Templates" sub-folder. It is also available to ISE Staff on the **J Drive** in the **Regulation SCI** folder / "**Toolkit**" sub-folder**.**

[210] See Adopting Release at p. 408
[211] See 17 CFR 240.24b-2.
[212] See Adopting Release at p. 424.

The **ISE Internal SCI Event Reporting Template**, or similar document (*e.g.*, the post mortem document), prepared during the SCI Event incident management process as described in *SCI Event Incident Management Process*, above, is designed to capture the required Rule 1002(b)(2)(i) and 1002(b)(2)(ii) information and should be utilized as an efficient information source for Exhibit 1 to Form SCI.

Pursuant to the requirements of Rule 1002(b)(2), within 24 hours of notifying the Commission of the occurrence of the SCI Event, as described above, the ISE Compliance Officer or General Counsel shall file Form SCI with the Commission, attaching Exhibit 1, *Rule 1002(b)(2) Notification of SCI Event*, as required.

a) Good Faith, Best Efforts Basis Standard: 24-Hour Written Notification

Rule 1002(b)(2), *Obligations related to SCI events – Commission notification and recordkeeping of SCI events*, requires that the 24-hour written notification be made on a good faith, best efforts basis. This standard acknowledges that a written notification provided within 24 hours may provide only a preliminary assessment of the SCI Event, that additional information may come to light after the initial 24-hour period, and that the initial assessment may prove, in retrospect, to be incorrect or incomplete.

The good faith, best efforts standard does not require that the written notification be a comprehensive or complete assessment of the SCI Event unless, of course, ISE has completed a full assessment by the time of the 24-hour notification requirement.

- A "good faith" standard will help to ensure that ISE will not be accountable for unintentional inaccuracies or omissions contained in its 24-hour notification to the Commission.

- A "best efforts" standard will help to ensure that ISE will make a diligent and timely attempt to provide all the information required by the 24-hour written notification requirement.[213]

Consistent with the requirements of Rule 1002(b)(2), and pursuant to the SCI Event incident management procedures described in *SCI Event Incident Management Process*, above, the relevant incident management team will promptly prepare the **ISE Internal SCI Event Reporting Template**, or similar document (*e.g.*, the post mortem document), with the information known at the time, even if only preliminary, and submit to the Responsible SCI Personnel and the ISE Compliance Officer to facilitate the 24-hour written notification requirement. The 24-hour written notification to the Commission shall be filed by the ISE Compliance Officer or General Counsel.

3. REGULAR UPDATES TO COMMISSION: RULE 1002(b)(3)

To permit the Commission to fully monitor the SCI Event,[214] Rule 1002(b)(3), *Obligations related to SCI events – Commission notification and recordkeeping of SCI events*, requires that ISE shall, until such time as the SCI Event is resolved and ISE's investigation of the SCI Event is closed, provide updates pertaining to such SCI Event to the Commission on a regular basis, or at such frequency as reasonably requested by a representative of the Commission, to correct any materially incorrect information previously provided,

[213] See Adopting Release at pp. 287-88.
[214] See Adopting Release at p. 295.

or when new material information is discovered, including but not limited to, any of the information listed in Rule 1002(b)(2)(ii).[215] Although it is not required, Commission Staff encourages SCI Entities to make use of Form SCI in providing regular updates, when appropriate, as it provides a standardized means for submitting such updates to the Commission.[216] The use of Form SCI also permits ISE to electronically request confidential treatment of all information filed on Form SCI.[217]

Form SCI. Rule 1002(b)(3) allows ISE to discuss the update with Commission Staff orally (via the designated phone number listed below, or by email via the designated email listed below), rather than by completing Form SCI, although ISE may use Form SCI if it chooses to do so.[218] If ISE chooses to utilize Form SCI to submit a Rule 1002(b)(3) update, ISE will be able to submit a short description of the update and attach documents regarding such update as part of Exhibit 6, *Optional Attachments*, to Form SCI,[219] as well as request confidential treatment of all information contained on Form SCI.[220]

Pursuant to the SCI Event incident management procedures described in *SCI Event Incident Management Process*, above, the relevant incident management team may update and submit the **ISE Internal SCI Event Reporting Template**, or similar document (*e.g.*, the post mortem document), to the Responsible SCI Personnel and ISE Compliance Officer on a regular basis, or upon request, to correct any materially incorrect information previously provided, or when new material information is discovered. Pursuant to Rule 1002(b)(3), the ISE Compliance Officer or General Counsel shall update the Commission, as required.

Note: With respect to the Form SCI submissions where the rules do not specifically provide for updates – *i.e.*, interim SCI Event notifications under Rule 1002(b)(4), quarterly de minimis SCI Event notifications under Rule 1002(b)(5), report of SCI Reviews under Rule 1003(b)(3)) – if ISE discovers that a previously submitted Form SCI must be corrected or updated, ISE should contact Commission Staff as it corrects or updates the prior submission.[221]

Notification	Commission Contact
Oral/Telephone	**202 551-6300**.
Email	**cyberwatch@sec.gov**

As advised by Commission Staff during the **Cyber Watch Call**,[222] a team of analysts are available to answer the phone **30 minutes prior to market open** and **30 minutes after market close**. During other times, ISE can leave a voicemail for any oral notification.

Confidential Treatment Requests. For any emailed notifications, ISE must make a confidential treatment request in paper format only,[223] pursuant to Rule 24b-2 under the Exchange Act.[224]

---

[215] See *24-Hour Written Notification: Rule 1002(b)(2)*, above.
[216] See Regulation SCI FAQs at: http://www.sec.gov/divisions/marketreg/regulation-sci-faq.shtml
[217] See Regulation SCI FAQs.
[218] See Adopting Release at p. 419, FN 1289.
[219] See Adopting Release at p. 424.
[220] See Adopting Release at p. 408.
[221] See Adopting Release at P. 420.
[222] October 27, 2015 conference call between ISE and the Commission's Cyber Watch Team.
[223] See Adopting Release at p. 408
[224] See 17 CFR 240.24b-2.

Secondary (additional) Notification. The Commission has indicated, in the Regulation SCI FAQs, that, as a secondary notification, ISE **may** *additionally* notify any other Commission Staff it feels appropriate, including any Commission Staff member with whom ISE's personnel consults regarding the issues relating to a given SCI Event.

4. FINAL WRITTEN NOTIFICATION: RULE 1002(b)(4)(i)(A)

ISE's Rule 1002(b) reporting obligations concerning an SCI Event are completed when ISE submits a final written notification to the Commission via Form SCI, as required by Rule 1002(b)(4).[225] Final written Commission notification is not required until the resolution of the SCI Event and the completion of ISE's investigation of the SCI Event.[226]

Pursuant to Rule 1002(b)(4)(i)(A), *Obligations related to SCI events – Commission notification and recordkeeping of SCI events*, if an SCI Event is resolved and ISE's investigation of the SCI Event is closed within 30 calendar days of the occurrence of the SCI Event, then within five business days after the resolution of the SCI Event and closure of the investigation regarding the SCI Event, ISE must submit a final written notification pertaining to such SCI Event to the Commission containing the information required in Rule 1002(b)(4)(ii).

Form SCI. Under Rule 1002(b)(4)(ii), ISE is required to provide the following information in Exhibit 2, *Rule 1002(b)(4) Final or Interim Report of SCI Event*, to Form SCI (and also indicate whether it is a final report or an interim status report[227]):

- Rule 1002(b)(4)(ii)(A): A detailed description of:
  - ISE's assessment of the types and number of market participants affected by the SCI Event;
  - ISE's assessment of the impact of the SCI Event on the market;
  - the steps ISE has taken, is taking, or plans to take, with respect to the SCI Event;
  - the time the SCI Event was resolved;
  - ISE's rule(s) and/or governing document(s), as applicable, that relate to the SCI Event; and
  - any other pertinent information known by ISE about the SCI Event;

- Rule 1002(b)(4)(ii)(B): A copy of any information disseminated pursuant to Rule 1002(c), *Dissemination of SCI events*,[228] by ISE to date regarding the SCI Event to any of its members or participants; and

[225] See Adopting Release at p. 298.
[226] See Adopting Release at p. 407.
[227] See Adopting Release at p. 424.
[228] See *Dissemination of SCI Events: Rule 1002(c)*, below.

- Rule 1002(b)(4)(ii)(C): An analysis of parties that may have experienced a loss, whether monetary or otherwise, due to the SCI Event, the number of such parties, and an estimate of the aggregate amount of such loss.[229]

Pursuant to the SCI Event incident management procedures described in *SCI Event Incident Management Process*, above, the relevant incident management team shall submit the final updated **ISE Internal SCI Event Reporting Template**, or similar document (*e.g.*, the post mortem document), to the Responsible SCI Personnel and ISE Compliance Officer when the SCI Event has been resolved and closed. The ISE Compliance Officer or General Counsel will file Form SCI, along with Exhibit 2, *Rule 1002(b)(4) Final or Interim Report of SCI Event*, with the Commission.

The information in the final written notification should provide the Commission with a comprehensive analysis to more fully understand and assess the impact caused by the SCI Event.[230]

The Exhibit 2, *Rule 1002(b)(4) Final or Interim Report of SCI Event* Template is stored in the **Compliance Department Shared Drive** in the "Templates" sub-folder. It is also available to ISE Staff on the **J Drive** in the **Regulation SCI** folder / "**Toolkit**" sub-folder**.**

5. INTERIM WRITTEN NOTIFICATION: RULE 1002(b)(4)(i)(B)(1), RULE 1002(b)(4)(i)(B)(2)

If, within 30 calendar days of the occurrence of the SCI Event, the SCI Event has not been resolved, ISE must, within those 30 calendar days, submit an interim written notification to the Commission (in lieu of the final written report described above) as well as a subsequent final written report when the SCI Event is finally resolved, as described below.

a) SCI Event Not Closed Within 30 Calendar Days of Occurrence: Interim Written Notification.

Pursuant to Rule 1002(b)(4)(i)(B)(1), *Obligations related to SCI events – Commission notification and recordkeeping of SCI events*, if an SCI Event is not resolved or ISE's investigation of the SCI Event is not closed within **30** calendar days of the occurrence of the SCI Event, ISE must submit an interim written notification pertaining to such SCI Event to the Commission within 30 calendar days after the occurrence of the SCI Event containing the information required in Rule 1002(b)(4)(ii), above, to the extent known at the time.

Form SCI. Under Rule 1002(b)(4)(ii), ISE is required to provide the following information in Exhibit 2, *Rule 1002(b)(4) Final or Interim Report of SCI Event*, to Form SCI (and also indicate whether it is a final report or an interim status report[231]):

[229] See Adopting Release at p. 425.
[230] See Adopting Release at p. 462.
[231] See Adopting Release at p. 424.

- Rule 1002(b)(4)(ii)(A): A detailed description of:
  - ISE's assessment of the types and number of market participants affected by the SCI Event;
  - ISE's assessment of the impact of the SCI Event on the market;
  - the steps ISE has taken, is taking, or plans to take, with respect to the SCI Event;
  - the time the SCI Event was resolved;
  - ISE's rule(s) and/or governing document(s), as applicable, that relate to the SCI Event; and
  - any other pertinent information known by ISE about the SCI Event;

- Rule 1002(b)(4)(ii)(B): A copy of any information disseminated pursuant to Rule 1002(c), *Dissemination of SCI events*,[232] by ISE to date regarding the SCI Event to any of its members or participants; and

Rule 1002(b)(4)(ii)(C): An analysis of parties that may have experienced a loss, whether monetary or otherwise, due to the SCI Event, the number of such parties, and an estimate of the aggregate amount of such loss.[233]

Pursuant to the SCI Event incident management procedures described in *SCI Event Incident Management Process*, above, the relevant incident management team shall update and submit the **ISE Internal SCI Event Reporting Template**, or similar document (*e.g.*, the post mortem document), to the Responsible SCI Personnel and ISE Compliance Officer on a regular basis, or upon request, to correct any materially incorrect information previously provided, or when new material information is discovered.

Pursuant to Rule 1002(b)(4)(i)(B)(1), the ISE Compliance Officer or General Counsel will submit the interim written notification to the Commission by filing Form SCI and attaching Exhibit 2, *Rule 1002(b)(4) Final or Interim Report of SCI Event*, as required.

The Exhibit 2, *Rule 1002(b)(4) Final or Interim Report of SCI Event* Template is stored in the **Compliance Department Shared Drive** in the "Templates" sub-folder. It is also available to ISE Staff on the **J Drive** in the **Regulation SCI** folder / "**Toolkit**" sub-folder**.**

b) SCI Event Not Closed Within 30 Calendar Days of Occurrence: Final Written Notification.

Pursuant to Rule 1002(b)(4)(i)(B)(2), *Obligations related to SCI events – Commission notification and recordkeeping of SCI events*, within five business days after the resolution of such SCI Event and closure of the investigation regarding such SCI Event, ISE must submit a final written notification pertaining to such SCI Event to the Commission containing the information required in Rule 1002(b)(4)(ii), above.

Form SCI. Under Rule 1002(b)(4)(ii), ISE is required to provide the following information in Exhibit 2, *Rule 1002(b)(4) Final or Interim Report of SCI Event*, to Form SCI (and also indicate whether it is a final report or an interim status report[234]):

---

[232] See *Dissemination of SCI Events: Rule 1002(c)*, below.
[233] See Adopting Release at p. 425.
[234] See Adopting Release at p. 424.

- Rule 1002(b)(4)(ii)(A): A detailed description of:
  - ISE's assessment of the types and number of market participants affected by the SCI Event;
  - ISE's assessment of the impact of the SCI Event on the market;
  - the steps ISE has taken, is taking, or plans to take, with respect to the SCI Event;
  - the time the SCI Event was resolved;
  - ISE's rule(s) and/or governing document(s), as applicable, that relate to the SCI Event; and
  - any other pertinent information known by ISE about the SCI Event;

- Rule 1002(b)(4)(ii)(B): A copy of any information disseminated pursuant to Rule 1002(c), *Dissemination of SCI events*,[235] by ISE to date regarding the SCI Event to any of its members or participants; and

Rule 1002(b)(4)(ii)(C): An analysis of parties that may have experienced a loss, whether monetary or otherwise, due to the SCI Event, the number of such parties, and an estimate of the aggregate amount of such loss.[236]

Pursuant to the SCI Event incident management procedures described in *SCI Event Incident Management Process*, above, the relevant incident management team shall submit the final updated **ISE Internal SCI Event Reporting Template**, or similar document (*e.g.*, the post mortem document), to the Responsible SCI Personnel and ISE Compliance Officer when the SCI Event has been resolved and closed.

Pursuant to Rule 1002(b)(4)(i)(B)(2), the ISE Compliance Officer or General Counsel will submit the final written notification to the Commission by filing Form SCI and attaching Exhibit 2, *Rule 1002(b)(4) Final or Interim Report of SCI Event*, as required. The Exhibit 2, *Rule 1002(b)(4) Final or Interim Report of SCI Event* Template is stored in the **Compliance Department Shared Drive** in the "Templates" sub-folder. It is also available to ISE Staff on the **J Drive** in the **Regulation SCI** folder / "**Toolkit**" sub-folder**.**

The information in the written notification should provide the Commission with a comprehensive analysis to more fully understand and assess the impact caused by the SCI Event.[237]

C. Commission Notification and Recordkeeping of De Minimis SCI Events: Rule 1002(b)(5)

De Minimis SCI Events are not subject to immediate Commission notification. Instead, all De Minimis SCI Events are subject to recordkeeping requirements, while de minimis Systems Disruptions and de minimis Systems Intrusions are subject to a quarterly reporting obligation, as set forth in Rule 1002(b)(5), *Obligations related to SCI events – Commission notification and recordkeeping of SCI events*.[238]

[235] See *Dissemination of SCI Events: Rule 1002(c)*, below.
[236] See Adopting Release at p. 425.
[237] See Adopting Release at p. 462.
[238] See Adopting Release at p. 259.

Pursuant to Rule 1002(b)(5), the requirements of Rules 1002(b)(1) through 1002(b)(4) shall not apply to any SCI Event that has had, or ISE reasonably estimates would have, no or a de minimis impact on ISE's operations or on market participants. For such events, ISE shall:

- Rule 1002(b)(5)(i): Make, keep, and preserve records relating to all such SCI Events; and

- Rule 1002(b)(5)(ii): Submit to the Commission a report, within 30 calendar days after the end of each calendar quarter, containing a summary description of such Systems Disruptions and Systems Intrusions, including the SCI Systems and, for Systems Intrusions, Indirect SCI Systems, affected by such Systems Disruptions and Systems Intrusions during the applicable calendar quarter.

1. RECORDKEEPING REQUIREMENT: RULE 1002(b)(5)(i)

Rule 1002(b)(5)(i), *Obligations related to SCI events – Commission notification and recordkeeping of SCI events*, requires ISE to make, keep, and preserve records relating to all De Minimis SCI Events.

ISE's *Record Retention Policy* describes ISE's record retention obligations and sets forth ISE's procedures for proper creation, maintenance and preservation of documents. Pursuant to the *Record Retention Policy*, all documents pertaining to ISE's

business and self-regulatory functions must be retained.

As described in *Recordkeeping Requirements*, below, ISE's *Record Retention Policy* is consistent with the requirements of Rule 1005, *Recordkeeping requirements related to compliance with Regulation SCI*, which requires ISE to make, keep, and preserve all documents relating to its compliance with Regulation SCI as prescribed in §240.17a-1[239] of the Securities Exchange Act.

Pursuant to the SCI Event incident management procedures described in *SCI Event Incident Management Process*, above, and consistent with the requirements of Rule 1002(b)(5)(i), the relevant incident management teams shall maintain records relating to all De Minimis SCI Events.

2. QUARTERLY REPORTING: RULE 1002(b)(5)(ii)

Rule 1002(b)(5)(ii), *Obligations related to SCI events – Commission notification and recordkeeping of SCI events*, requires that ISE submit to the Commission a report, within **30** calendar days after the end of each calendar quarter, containing a summary description of such [de minimis] Systems Disruptions and Systems Intrusions, including the SCI Systems and, for Systems Intrusions, Indirect SCI Systems, affected by such Systems Disruptions and Systems Intrusions during the applicable calendar quarter.

Pursuant to the SCI Event incident management procedures described in *SCI Event Incident Management Process*, above, and consistent with the requirements of Rule 1002(b)(5)(ii), the relevant incident management teams shall, within **15** calendar days after the end of each calendar quarter, submit a

[239] 17 CFR 240.17a-1, *Recordkeeping rule for national securities exchanges, national securities associations, registered clearing agencies and the Municipal Securities Rulemaking Board*.

summary description of any De Minimis SCI Events that occurred during such calendar quarter, including the SCI Systems affected, to the ISE Compliance Officer and Responsible SCI Personnel.

The 15 calendar day internal submission requirement facilitates any necessary internal follow up and the timely preparation of the **ISE Quarterly De Minimis SCI Events Report** for submission as Exhibit 3 to Form SCI, as described below. The template for the **ISE Quarterly De Minimis SCI Events Report** is stored in the **Compliance Department Shared Drive** in the "Templates" sub-folder**.** It is also available to ISE Staff on the **J Drive** in the **Regulation SCI** folder / "**Toolkit**" sub-folder**.**

Form SCI. Pursuant to the requirements of Rule 1002(b)(5)(ii), the ISE Compliance Officer or General Counsel shall file Form SCI along with Exhibit 3, *Rule 1002(b)(5)(ii) Quarterly Report of De Minimis SCI Events*, within 30 calendar days after the end of the calendar quarter, with the Commission. For any calendar quarter for which there were no De Minimis SCI Events, Form SCI shall be filed with Exhibit 3 indicating that there were no De Minimis SCI Events during the calendar quarter.

D. DISSEMINATION OF SCI EVENTS: RULE 1002(c)

In addition to notifying the Commission about the occurrence of SCI Events (Rule 1002(b)), pursuant to Rule 1002(c), *Obligations related to SCI events – Dissemination of SCI events*, ISE must also disseminate information about such events to its members or participants, with certain exceptions, as described below.

The requirements of Rule 1002(c) address to whom and when ISE is obligated, under Regulation SCI, to disseminate information about the occurrence of SCI Events. However, subject to any applicable laws or regulations, ISE still retains the flexibility to disseminate information – *e.g.*, to members or participants, the public, or market participants that interact with the affected SCI Systems – at any time ISE determines to be appropriate.[240]

ISE would also be required to submit the disseminated information to the Commission as part of the report submitted pursuant to Rule 1002(b)(4),[241] as described in *Final Written Notification: Rule 1002(b)(4)(i)(A)*, and *Interim Written Notification: Rule 1002(b)(4)(i)(B)(1), Rule 1002(b)(4)(i)(B)(2),* above.

A Note On Dissemination Concerning SCI Events Affecting Third Party SCI Systems Operated on Behalf of ISE.

- **FINRA:** Pursuant to Rule 1002(c)(4)(i), which excepts market regulation or market surveillance systems from Rule 1002(c), *Dissemination of SCI events*, SCI Events impacting SCI Systems operated by FINRA on behalf of ISE are not subject to the dissemination requirement. This exception is also documented in FINRA's *Framework for Managing SCI Workflow under RSAs* term sheet, stored on the Compliance Department's shared drive.

[240] See Adopting Release at p. 325.
[241] See Adopting Release at p. 321, FN 983.

- **EXEGY:** For SCI Events impacting SCI Systems operated by Exegy on behalf of ISE, ISE is responsible for, and will disseminate, the required information based upon what is reported to ISE by Exegy via the **ISE SCI Event Notification Form**, stored on the Compliance shared drive in the "Templates" sub-folder**.** It is also available to ISE Staff on the **J Drive** in the **Regulation SCI** folder / "**Toolkit**" sub-folder**.**

1. DISSEMINATION PURSUANT TO A SYSTEMS DISRUPTION OR SYSTEMS COMPLIANCE ISSUE: RULE 1002(C)(1)

Rule 1002(c)(1), *Obligations related to SCI events – Dissemination of SCI events,* generally addresses dissemination requirements for Systems Disruptions and Systems Compliance Issues (only), unless an exception applies, as described in *Exceptions to Dissemination Requirement*, below.

Pursuant to Rule 1002(c)(1), ISE shall:

- Rule 1002(c)(1)(i): Promptly after any Responsible SCI Personnel has a reasonable basis to conclude that an SCI Event that is a Systems Disruption or Systems Compliance Issue has occurred, disseminate the following information about such SCI Event:
  - Rule 1002(c)(1)(i)(A): The system(s) affected by the SCI Event; and
  - Rule 1002(c)(1)(i)(B): A summary description of the SCI Event; and

- Rule 1002(c)(1)(ii): When known, promptly further disseminate the following information about such SCI Event:
  - Rule 1002(c)(1)(ii)(A): A detailed description of the SCI Event;
  - Rule 1002(c)(1)(ii)(B): ISE's current assessment of the types and number of market participants potentially affected by the SCI Event; and
  - Rule 1002(c)(1)(ii)(C): A description of the progress of its corrective action for the SCI Event and when the SCI Event has been or is expected to be resolved; and

- Rule 1002(c)(1)(iii): Until resolved, provide regular updates of any information required to be disseminated under Rules 1002(c)(1)(i) and 1002(c)(1)(ii).

Rule 1002(c)(1) strikes an appropriate balance by requiring ISE to disseminate specific information about SCI Events, but also permits ISE to have time to check relevant facts before disseminating that information.[242] Implicit in Rule 1002(c)(1)(iii)'s requirement to provide regular updates is that the disseminated information be accurate.[243]

[242] See Adopting Release at p. 315.

[243] See Adopting Release at p. 314. Without the dissemination of accurate information the impact on ISE's members or participants or the market may be more pronounced because market participants may not recognize that an SCI Event is occurring, or may mistakenly attribute unusual market activity to some other cause. See Adopting Release at p. 314.

The information required to satisfy the dissemination requirements of Rule 1002(c)(1) shall be provided to the ISE Compliance Officer through the SCI Event incident management procedures, described in *SCI Event Incident Management Process*, above.

Consistent with the requirements of Rule 1002(c)(1), ISE shall post a **Regulation SCI Notice** containing the information required to be disseminated by Rule 1002(c)(1) to a password-protected Regulation SCI page on its website for access by all ISE members. Prior to posting, the ISE Compliance Officer or Legal Department will review and approve the notice.

2. DISSEMINATION PURSUANT TO A SYSTEMS INTRUSION: RULE 1002(c)(2)

Rule 1002(c)(2), *Obligations related to SCI events – Dissemination of SCI events,* addresses dissemination requirements for Systems Intrusions (only). The content of the required disclosure for a Systems Intrusion is less detailed than required for other types of SCI Events.[244]

Pursuant to Rule 1002(c)(2), ISE shall, promptly after any Responsible SCI Personnel has a reasonable basis to conclude that a SCI Event that is a Systems Intrusion has occurred, disseminate a summary description of the Systems Intrusion, including

- a description of the corrective action taken by ISE and
- when the Systems Intrusion has been or is expected to be resolved,
    - unless ISE determines that dissemination of such information would likely compromise the security of ISE's SCI Systems or Indirect SCI Systems, or an investigation of the Systems Intrusion, and documents the reasons for such determination.

When ISE determines that a Systems Intrusion has occurred, the **Information Security Director or Department Head** is responsible for determining whether prompt dissemination of information concerning the Systems Intrusion, as required by Rule 1002(c)(2), should be delayed for security purposes. To the extent the Information Security Director or Department Head determines that, for security purposes, dissemination should be delayed, the Information Security Director or Department Head shall document the reason for such determination and provide a copy to the ISE Compliance Officer. Such documentation shall be maintained in accordance with the recordkeeping requirements in Section XI, *Recordkeeping Requirements*, below.

If the Information Security Director or Department Head cannot (or can no longer) determine that information dissemination as required by Rule 1002(c)(2) would likely compromise the security of ISE's SCI Systems or Indirect SCI Systems, or an investigation of the Systems Intrusion, no delay (or further delay, if applicable) in dissemination is permitted.[245] Therefore, the Information Security Director or Department Head shall promptly advise the ISE Compliance Officer when dissemination of information concerning such Systems Intrusion will no longer pose a security risk to ISE's SCI Systems or Indirect SCI Systems, in which instance, ISE shall disseminate the information as required by Rule 1002(c)(2).

[244] See Adopting Release at p. 316.
[245] See Adopting Release at pp. 316-17.

Pursuant to Rule 1002(c)(2), information about a Systems Intrusion is required to be disseminated eventually, as circumstances permitting a delay (*i.e.*, dissemination of information would likely compromise the security of ISE's SCI Systems or Indirect SCI Systems, or an investigation of the Systems Intrusion), will not continue indefinitely.[246]

The information required to satisfy the dissemination requirements of Rule 1002(c)(2) shall be provided to the ISE Compliance Officer through the SCI Event incident management procedures, described in *SCI Event Incident Management Process*, above.

Consistent with the requirements of Rule 1002(c)(2), ISE shall post a **Regulation SCI Notice** containing the information required to be disseminated by Rule 1002(c)(2) to a password-protected Regulation SCI page on its website for access by all ISE members. Prior to posting, the ISE Compliance Officer or Legal Department will review and approve the notice.

3. Dissemination to Affected Members Only (for other than Major SCI Events): Rule 1002(c)(3)

Pursuant to **Rule 1002(c)(3),** *Obligations related to SCI events – Dissemination of SCI events*, the information required to be disseminated under Rules 1002(c)(1) and 1002(c)(2) promptly after any Responsible SCI Personnel has a reasonable basis to conclude that an SCI Event has occurred, shall be

- promptly disseminated by ISE to those members or participants of ISE that any Responsible SCI Personnel has reasonably estimated may have been affected by the SCI Event, and
- promptly disseminated to any additional members or participants that any Responsible SCI Personnel subsequently reasonably estimates may have been affected by the SCI Event;
- provided, however, that for Major SCI Events, the information required to be disseminated under Rules 1002(c)(1) and 1002(c)(2) shall be promptly disseminated by ISE to all of its members or participants.

The requirement for prompt dissemination, as opposed to immediate dissemination, is designed to provide some limited flexibility to ISE to determine an efficient way to disseminate information to multiple potentially affected members or participants, or all of its members or participants, as the case may be, in a timely manner. Likewise, as new information becomes known, immediate updates are not required, but ISE is obligated to also disseminate updated information "promptly" after it is known.[247]

The information required to satisfy the dissemination requirements of Rule 1002(c)(3) shall be provided to the ISE Compliance Officer through the SCI Event incident management procedures, described in *SCI Event Incident Management Process*, above.

Consistent with the requirements of Rule 1002(c)(3), ISE shall post a **Regulation SCI Notice** containing the information required to be disseminated by Rule 1002(c)(3) to a password-protected Regulation SCI page

[246] See Adopting Release at p. 317.
[247] See Adopting Release at p. 315.

on its website for access by all ISE members. Prior to posting, the ISE Compliance Officer or Legal Department will review and approve the notice.

4. Dissemination to All Members (for Major SCI Events): Rule 1002(c)(3)

As stated above, Rule 1002(c)(3), *Obligations related to SCI events – Dissemination of SCI events*, requires that for Major SCI Events, the information required to be disseminated under Rules 1002(c)(1) and 1002(c)(2) shall be promptly disseminated by ISE to all of its members or participants.

Rule 1002(c)(3) does not specify how ISE is to disseminate information to all of its members or participants when required to do so, but the Commission believes that posting the information on a website accessible to, at a minimum, all of ISE's members or participants (*e.g.*, on a "systems status alerts" page) would meet the rule's requirements.[248]

Irrespective of the medium ISE chooses to disseminate information to ISE members or participants, ISE would also be required to submit the disseminated information to the Commission as part of the report submitted pursuant to Rule 1002(b)(4),[249] as described in *Final Written Notification: Rule 1002(b)(4)(i)(A)*, and *Interim Written Notification: Rule 1002(b)(4)(i)(B)(1), Rule 1002(b)(4)(i)(B)(2),* above.

The information required to satisfy the dissemination requirements of Rule 1002(c)(3) shall be provided to the ISE Compliance Officer through the SCI Event incident management procedures, described in *SCI Event Incident Management Process*, above.

Consistent with the requirements of Rule 1002(c)(3), ISE shall post a **Regulation SCI Notice** containing the information required to be disseminated by Rule 1002(c)(3) to a password-protected Regulation SCI page on its website for access by all ISE members. Prior to posting, the ISE Compliance Officer or Legal Department will review and approve the notice.

5. Exceptions to Dissemination Requirement

Regulation SCI provides certain exceptions to the dissemination requirement for SCI Events that are Systems Intrusions, and SCI Events affecting ISE Market Regulation and Market Surveillance systems.

a) Dissemination Exception for Systems Intrusions: Rule 1002(c)(2)

As described in *Dissemination Pursuant to a Systems Intrusion: Rule 1002(c)(2)*, above, although ISE is required to disseminate information concerning Systems Intrusions, Rule 1002(c)(2), *Obligations related to SCI events – Dissemination of SCI events*, provides an exception to the information dissemination requirement for Systems Intrusions when ISE determines that dissemination of information would likely compromise the security of ISE's systems, or an investigation of the Systems Intrusion, and ISE documents the reasons for such determination.[250] However, this exception only lasts until it is determined that

[248] See Adopting Release at pp. 320-21.
[249] See Adopting Release at p. 321, FN 983.
[250] See Adopting Release at pp. 456-57.

information dissemination concerning the Systems Intrusion will no longer compromise such security or investigation. As described in *Obligations related to SCI events – Dissemination of SCI events*, above, the Information Security Director or Department Head is responsible for determining whether prompt dissemination of information concerning the Systems Intrusion, as required by Rule 1002(c)(2), should be delayed for security purposes.

b) Dissemination Exception for SCI Events Relating to Market Regulation or Market Surveillance Systems: Rule 1002(c)(4)(i)

Pursuant to Rule 1002(c)(4)(i), *Obligations related to SCI events – Dissemination of SCI events*, the requirements of Rules 1002(c)(1) through 1002(c)(3) shall not apply to SCI Events to the extent they relate to market regulation or market surveillance systems. The reason for this exception is that dissemination of such information to ISE's members or participants or the public at large could encourage prohibited market activity.[251]

However, for purposes of clarification, the dissemination exception for market regulation or market surveillance systems is limited to dissemination of information about SCI Events related to market regulation or market surveillance systems. Information about an SCI Event that impacts other ISE SCI Systems would still be required to be disseminated in accordance with Rule 1002(c) *even if* that same SCI Event also impacts ISE Market Regulation or Market Surveillance systems.[252]

The information required to satisfy the dissemination requirements of Rule 1002(c)(4)(i) shall be provided to the ISE Compliance Officer through the SCI Event incident management procedures, described in *SCI Event Incident Management Process*, above.

Consistent with the requirements of Rule 1002(c)(4)(i), ISE shall post a **Regulation SCI Notice** containing the information required to be disseminated by Rule 1002(c)(4)(i) to a password-protected Regulation SCI page on its website for access by all ISE members. Prior to posting, the ISE Compliance Officer or Legal Department will review and approve the notice.

c) Dissemination Exception for De Minimis SCI Events: Rule 1002(c)(4)(ii)

Pursuant to Rule 1002(c)(4)(ii), *Obligations related to SCI events – Dissemination of SCI events*, the requirements of Rules 1002(c)(1) through 1002(c)(3) shall not apply to any SCI Event that has had, or ISE reasonably estimates would have, no or a de minimis impact on ISE's operations or on market participants.

The exception in Rule 1002(c)(4)(ii) for De Minimis SCI Events is consistent with the Commission's approach to excluding De Minimis SCI Events from the immediate Commission notification requirements in Rule 1002(b), *Obligations related to SCI events – Commission notification and recordkeeping of SCI events*.[253]

---

[251] See Adopting Release at p. 323.
[252] See Adopting Release at pp. 323-24.
[253] See Adopting Release at p. 324.

6. RULE 1002(C) DISSEMINATION SUMMARY

Below is a summary of the Rule 1002(c) Information Dissemination Requirements:

- Prompt Initial Dissemination Requirements (excluding De Minimis SCI Events) – Rule 1002(c)(1)(i)
  - *System(s) Affected by SCI Event – Rule 1002(c)(1)(i)(A)*
  - *Summary Description of SCI Event – Rule 1002(c)(1)(i)(B)*

- Additional Dissemination Requirements, *when known* – Rule 1002(c)(1)(ii)
  - *Detailed Description of SCI Event – Rule 1002(c)(1)(ii)(A)*
  - *Current Assessment of the Types and Number of Potentially Affected Market Participants – Rule 1002(c)(1)(ii)(B)*
  - *Progress of Corrective Action and Resolution, or Expected Resolution, of SCI Event – Rule 1002(c)(1)(ii)(c)*

- Regular Updates Until Resolution - Rule 1002(c)(1)(iii)
  - *Until Resolved, Regular Updates of Any 1002(c)(1)(i) and (c)(1)(ii) Required Information*

INTENTIONALLY LEFT BLANK

VIII. MATERIAL SCI SYSTEMS CHANGES

Rule 1003(a), *Obligations related to systems changes; SCI review – Systems changes*, requires ISE to notify the Commission, on a quarterly basis, of material changes to its SCI Systems and establish written criteria for identifying which changes to its SCI Systems are material systems changes for purposes of this reporting requirement. Rule 1003(a) also requires that ISE correct any material errors in, or material omissions from, a previously submitted report to the Commission.

Changes that are part of ISE's standard operations, or which are routinely performed without the need to change existing functionalities, are not considered changes to ISE's SCI Systems covered by the quarterly reporting requirement of Rule 1003(a).[254] The *ISE Change Management Policy & Process Document* documents ISE's system of internal controls over changes to SCI systems.

A. A NOTE ON INDIRECT SCI SYSTEMS AND DEVELOPMENT AND TESTING SYSTEMS

Indirect SCI Systems. To the extent that ISE determines that certain changes to the security of its Indirect SCI Systems are not material in accordance with its reasonably written criteria, such changes are not required to be reported to the Commission.[255]

Development and Testing Systems. As a rule, SCI Systems do not include development and testing systems. However, Indirect SCI Systems could include development and testing systems if they are not walled-off from SCI Systems. In these circumstances, Rule 1003(a)(1)'s quarterly notification requirement could apply to material changes to the *security* of development and testing systems that are not walled-off from SCI Systems.[256]

B. IDENTIFYING A MATERIAL SYSTEMS CHANGE: RULE 1003(a)(1):

Whether a systems change is material is dependent on the facts and circumstances, such as: (i) the reason for the change, and (ii) how it may impact operations.[257]

The Commission acknowledges that there currently is no industry definition of "material systems change" that is applicable to all SCI Entities that can serve as the basis for a precise definition of the term "material systems change" in Regulation SCI.[258] However, the Commission set forth examples in the SCI Proposal that it *preliminarily* believed could be included within the *proposed definition* of material systems change. These proposed, preliminary, examples included:[259]

- Major systems architecture changes;

[254] See Adopting Release at p. 222, FN 687.
[255] See Adopting Release at p. 345.
[256] See Adopting Release at p. 346.
[257] See Adopting Release at p. 345.
[258] See Adopting Release at pp. 344-45.
[259] See Adopting Release at p. 326, FN 995.

- Reconfiguration of systems that would cause a variation greater than five percent in throughput or storage;

- The introduction of new business functions or services;

- Changes to external interfaces;

- Changes that could increase susceptibility to major outages;

- Changes that could increase risks to data security;

- Changes that were, or would be, reported to or referred to the entity's board of directors, a body performing a function similar to the board of directors, or senior management; and

- Changes that could require allocation or use of significant resources.

The Adopting Release did not include a definition for material systems change. Instead, it cited the above-listed proposed definitions as examples.

Because SCI Entities differ in nature, size, technology, business model, and other aspects of their businesses,[260] the Commission acknowledges that an SCI Entity is in the best position to determine, in the first instance, whether a change (or **series of changes**), is material in the context of its own systems.[261] Therefore, if ISE reasonably believes that some of the examples of material systems changes identified in the SCI Proposal can appropriately serve as criteria for identifying material systems changes, and such criteria is set forth in ISE's reasonable written criteria, ISE may identify material systems changes in accordance with such written criteria.[262]

A Note on "Series of Changes": Some systems changes may not, by themselves, be considered material by ISE but, in the aggregate, can be considered material by ISE (*e.g.*, making a series of small systems changes over time in order to implement a broad systems change).[263]

1. ISE MATERIAL SYSTEMS CHANGE CRITERIA: RULE 1003(a)(1)

Rule 1003(a)(1), *Obligations related to systems changes; SCI review – Systems changes*, requires, in relevant part, that ISE shall establish reasonable written criteria for identifying a change to its SCI Systems and the security of Indirect SCI Systems as material and report such changes in accordance with such criteria.

[260] See Adopting Release at p. 344.
[261] See Adopting Release at p. 345.
[262] See Adopting Release at p. 346.
[263] See Adopting Release at p. 333.

As discussed above, ISE has reasonable discretion in establishing the written criteria in order to capture the systems changes that it believes are material.[264]

Consistent with the requirements of Rule 1003(a)(1), ISE has established the following reasonable written criteria for determining whether a systems change is material and, thus, is required to be reported to the Commission, quarterly, in the **ISE Material SCI Systems Change(s) Report**[265] attached to Form SCI as Exhibit 4, *Rule 1003(a) Quarterly Report of Systems Changes*.[266]

ISE Material Systems Change Criteria
Material systems architecture changes (includes "infrastructure" changes)
The introduction of new business functions or services, or material enhancements to existing functionality
Material changes to external interfaces
Changes that were, or would be, reported to or referred to ISE's Board of Directors that are not part of a routine/regular update

2. COMMISSION REVIEW OF ISE MATERIAL SYSTEMS CHANGE CRITERIA: RULE 1003(a)(1)

As with other policies and procedures under Regulation SCI, Commission Staff may review ISE's established criteria relating to the materiality of a systems change (*e.g.*, in the course of an examination) to determine whether it agrees with ISE's assessment that such criteria is reasonable and in compliance with the requirements of Rule 1003(a).[267]

C. COMMISSION NOTIFICATION OF MATERIAL SYSTEMS CHANGE(S): RULE 1003(a)(1)

Pursuant to Rule 1003(a)(1), *Obligations related to systems changes; SCI review – Systems changes*, ISE shall, within 30 calendar days after the end of each calendar quarter, submit to the Commission a report describing completed, ongoing, and planned material changes to its SCI Systems and the security of Indirect SCI Systems, during the prior, current, and subsequent calendar quarters, including the dates or expected dates of commencement and completion.

Note: The quarterly report must also include material systems changes that were implemented in response to exigent circumstances during the prior and current calendar quarters.[268]

---

[264] See Adopting Release at p. 345.
[265] See *ISE Material SCI Systems Change(s) Report*, below.
[266] See **Appendix J-2: Form SCI – Schedule of Exhibits**
[267] See Adopting Release at p. 347.
[268] See Adopting Release at p. 333.

The quarterly notification requirement will permit the Commission and its staff to have up-to-date information regarding ISE's systems development progress and plans, to aid in understanding the operations and functionality of the systems and any material changes thereto, without requiring ISE to submit a notification to the Commission for each material systems change.[269] In addition, to the extent the Commission seeks additional information about a given change noted in a quarterly report, ISE would be required to provide Commission Staff with such information in accordance with Rule 1005, *Recordkeeping requirements related to compliance with Regulation SCI*,[270] discussed in *Recordkeeping Requirements*, below.

To the extent certain material systems changes are related or similar, ISE will not be required to separately notify the Commission of each change. Instead, ISE can describe such related changes within the single quarterly report.[271] Further, for systems changes deployed by ISE that may not, by themselves, be considered material by ISE, but that, in the aggregate, can be considered material by ISE (*e.g.*, making a series of small systems changes over time in order to implement a broad systems change), such aggregate changes should be reported in the quarterly ISE Material SCI Systems Change(s) Report, discussed in *ISE Material SCI Systems Change(s) Report*, below, under Rule 1003(a)(1).[272]

1. QUARTERLY COMMISSION NOTIFICATION EXAMPLE: RULE 1003(a)(1)

The quarterly material systems change reports are required to include descriptions of material systems changes during the prior calendar quarter that were completed, ongoing, or planned.[273]

Therefore, if a report for the first quarter of a given year discusses ISE's plan to implement a particular series of material changes to an SCI System, Rule 1003(a)(1), *Obligations related to systems changes; SCI review – Systems changes*, requires that, in the report for the second quarter of that year, ISE describe the material systems changes that were completed, ongoing, and planned in the first quarter, including the planned changes discussed in the prior quarter's report, as applicable.[274]

Below is a Commission-provided example[275] of the quarterly reporting process using the calendar quarter ending December 31, 2014 as the quarter initiating the quarterly reporting process:

Quarter ending December 31, 2014 / January 30, 2015 ISE Material SCI Systems Change(s) Report. For the quarter ending December 31, 2014, ISE would be required to submit a report by January 30, 2015 (*i.e.*, within 30 calendar days after December 31, 2014) that describes material systems changes that ISE *has made* (including the dates when those changes commenced and were completed), *is currently implementing* (including the dates when those changes commenced and are expected to be completed), and *plans to make* (including the dates those changes are expected to commence and complete), for the

[269] See Adopting Release at p. 330.
[270] See Adopting Release at p. 338.
[271] See Adopting Release at p. 332.
[272] See Adopting Release at p. 332, FN 1012.
[273] See Adopting Release at p. 338.
[274] See Adopting Release at p. 338.
[275] See Adopting Release at p. 330, FN 1008.

period from October 1, 2014 (the *beginning of the prior calendar quarter*) through June 2015 (the *end of the subsequent calendar quarter*).

In this example, the next report that corresponds to the quarter ending March 31, 2015 would be required to be submitted by April 30, 2015.

Quarter ending March 31, 2015 / April 30, 2015 ISE Material SCI Systems Change(s) Report. In the April 30, 2015 report for the quarter ending March 31, 2015, ISE would be required to include descriptions of the material systems changes that were completed, ongoing, and planned in the quarter ending March 31, 2015, including the planned changes discussed in the January 30, 2015 report for the quarter ending December 31, 2014.

D. SUPPLEMENTAL MATERIAL SYSTEMS CHANGE NOTIFICATION: RULE 1003(a)(2)

Pursuant to Rule 1003(a)(2), *Obligations related to systems changes; SCI review – Systems changes*, ISE shall promptly submit a supplemental report notifying the Commission of a material error in or material omission from a report previously submitted under Rule 1003(a)(1).

In those instances where ISE realizes or discovers that information previously provided to the Commission in a quarterly report was inaccurate or that the quarterly report omitted information, the supplemental report requirement applies only if the error or omission in a prior report is **material**.[276]

Further, ISE must promptly submit the supplemental report to the Commission correcting such material inaccuracy or material omission because the Commission believes that it should, on an ongoing basis, have complete and correct information regarding material systems changes at an SCI Entity, rather than waiting until the next quarterly report to receive corrected information.[277]

E. ISE MATERIAL SCI SYSTEMS CHANGE(S) REPORT

Rule 1003(a)(1), *Obligations related to systems changes; SCI review – Systems changes*, specifically requires the quarterly reports to "describe" the material systems changes and the dates or expected dates of their commencement and completion, thereby giving ISE reasonable flexibility in determining precisely how to describe its material systems changes in the report in a manner that best suits the needs of ISE as well as the needs of the Commission and its staff.[278]

Consistent with Rule 1003(a)(1), the **ISE Material SCI Systems Change(s) Report** shall contain the following minimum information:

- The **date** of the **ISE Material SCI Systems Change(s) Report**: This date shall be no later than 30 calendar days after the end of the current calendar quarter being reported (*i.e.*, the deadline for submitting the report to the Commission as Exhibit 4, *Rule 1003(a) Quarterly Report of Systems Changes*, to Form SCI[279]).

[276] See Adopting Release at p. 348.
[277] See Adopting Release at p. 348.
[278] See Adopting Release at p. 338.
[279] See **Appendix J-1: Form SCI**, and **Appendix J-2: Form SCI – Schedule of Exhibits.**

- The **current calendar quarter** being reported: *i.e.*, "for calendar quarter ending ____."
- The **range/scope** of the **ISE Material SCI Systems Change(s) Report**: *i.e.*, date of 1st day of the *prior* calendar quarter through the date of the last day of the *subsequent* calendar quarter.
- Section on **Completed** Material Change(s) to ISE SCI Systems and the security of Indirect Systems: Include description of material systems change(s), date(s) commenced, and date(s) completed.
- Section on **In-Progress** Material Change(s) to ISE SCI Systems and the security of Indirect Systems: include description of material systems change(s), date(s) commenced, and expected completion date(s).
- Section on **Planned** Material Change(s) to ISE SCI Systems and the security of Indirect Systems: include description of material systems change(s), date(s) expected to commence, and expected completion date(s).

The **ISE Material SCI Systems Change(s) Report Template** is stored in the **Compliance Department Shared Drive** in the "Templates" sub-folder**.** It is also available to ISE Staff on the **J Drive** in the **Regulation SCI** folder / "**Toolkit**" sub-folder**.**

INTENTIONALLY LEFT BLANK

IX. AUDIT OBLIGATIONS

Regulation SCI requires ISE to perform periodic SCI Reviews in accordance with Rule 1003(b), *Obligations related to systems changes; SCI review – SCI review*. The SCI review should assist ISE in:

- assessing the effectiveness of its information technology practices, helping to ensure compliance with the safeguards provided by the requirements of Regulation SCI;
- identifying potential areas of weakness that require additional or modified controls; and
- determining where to best devote resources.[280]

The SCI Review is not a substitute for inspections and examinations conducted by Commission Staff, and ISE should expect that technology systems inspections and examinations will continue.[281]

ISE is also required to periodically review the effectiveness of Rule 1001, *Obligations related to policies and procedures of SCI entities,* policies and procedures in accordance with Rule 1001(a)(3), *Capacity, integrity, resiliency, availability, and security*; Rule 1001(b)(3), *Systems compliance*; and Rule 1001(c)(2), *Responsible SCI personnel*. These requirements are described below.

A. SCI REVIEW: RULE 1003(b)

Pursuant to Rule 1000, *Definitions*, SCI Review means a review, following established procedures and standards, that is performed by objective personnel having appropriate experience to conduct reviews of SCI Systems and Indirect SCI Systems, and which review contains:

- (1) A risk assessment with respect to such systems of ISE; and
- (2) An assessment of internal control design and effectiveness of its SCI Systems and Indirect SCI Systems to include logical and physical security controls, development processes, and information technology governance, consistent with industry standards.

SCI Reviews are to be performed by personnel of ISE or an external firm, provided that such personnel are, in fact objective and, as required by rule, have the appropriate experience to conduct reviews of SCI Systems and Indirect SCI Systems.[282]

- **Objective Personnel:** Objective personnel are those persons who have not been involved in the development, testing, or implementation of SCI Systems being reviewed. These personnel would be in a better position to identify weaknesses and deficiencies that were not identified in the development, testing and implementation stages.[283]
    - **Conflicts of Interest:** A person conducting an SCI Review should not have a conflict of interest that interferes with their ability to exercise judgment, express opinions, and

[280] See Adopting Release at p. 463.
[281] See Adopting Release at pp. 360-61.
[282] See Adopting Release at p. 350.
[283] See Adopting Release at p. 350.

present recommendations with impartiality.[284] Any personnel with conflicts of interest that have not been adequately mitigated to allow for objectivity should be excluded from serving in this role. SCI Entities can have appropriate policies and procedures in place to mitigate such conflicts or to help ensure that certain departments and/or specified personnel (such as internal audit departments) are appropriately insulated from such conflicts so as to be able to objectively conduct SCI Reviews.[285]

- **Experienced Personnel:** Experienced personnel have the knowledge and skills necessary to conduct SCI Reviews.[286]

Consistent with the requirements of Rule 1003(b) concerning objectivity and conflicts of interest (noted above), the *Internal Audit Charter – Deutsche Börse Group Policy Statement* (11 June 2015) (**Policy Statement-Internal Audit Charter**), which governs the internal audit departments of the respective Deutsche Börse Group entities, including ISE Internal Audit, includes a policy statement on auditor independence, objectivity and reporting line.[287] As documented in Section 4, *Independence, objectivity and reporting line* of the Policy Statement-Internal Audit Charter, the Head of ISE Internal Audit (Chief Internal Auditor) reports directly to the Audit Committee of ISE with an administrative reporting line to the General Counsel of ISE and a functional reporting line to the Head of Internal Audit DBAG.

Consistent with the requirements of Rule 1003(b) concerning experienced personnel (noted above), the Policy Statement-Internal Audit Charter includes a policy statement on responsibility which governs the competence of ISE internal auditors.[288]

SCI Reviews will be performed by ISE Internal Audit, unless use of external resources is deemed appropriate, pursuant to the Policy Statement-Internal Audit Charter, Section 5, *Responsibility*.

1. SCI REVIEW SCOPE: RULE 1003(b)

Regulation SCI permits ISE to design the scope and rigor of the SCI review for a particular SCI System based on its risk assessment of such system, provided that the SCI Review meets the requirements of the rule, such as:

- Including an assessment of internal control design and effectiveness to include:
  - Logical and physical security controls,
  - Development processes, and
  - Information technology governance, consistent with industry standards, and

- Performing penetration test reviews at least once every three (3) years.[289]

[284] See Adopting Release at p. 350.
[285] See Adopting Release at pp. 350-51.
[286] See Adopting Release at p. 350.
[287] See *Internal Audit Charter – Deutsche Börse Group Policy Statement* (11 June 2015), Section 4, *Independence, objectivity and reporting line*.
[288] See *Internal Audit Charter – Deutsche Börse Group Policy Statement* (11 June 2015), Section 5, *Responsibility*.
[289] See Adopting Release at p. 358.

Thus, ISE Internal Audit has the ability to design the specific parameters of an SCI Review within the confines of the general framework of the rule, including identifying its own review objectives and procedures, given its in-depth knowledge of, and familiarity with, ISE's systems and their attendant risks. The rule provides flexibility by permitting the review to be conducted "following established procedures and standards," which would be identified and established by ISE Internal Audit.[290]

Risk Assessment: A risk assessment is appropriate in order to determine the standards and requirements applicable to a given SCI System. ISE is required to conduct a risk-based assessment with regard to its SCI Systems and Indirect SCI Systems as part of its SCI Review at least annually.[291]

Consistent with the requirements of Rule 1003(b)(1), ISE Internal Audit uses a risk-based approach in defining specific areas of the organization to audit.[292] The ISE Risk Assessment methodology is included in the annual IT audit plan. The Head of ISE Internal Audit and ISE Internal Audit Director are responsible for the internal control risk assessments, audit plans, audit programs, and audit reports associated with IT. The ISE Audit Committee approves the risk assessment / audit plans annually.

2. SCI Review Frequency: Rule 1003(b)(1)

Rule 1003(b)(1), *Obligations related to systems changes; SCI review – SCI review*, requires ISE to conduct an SCI Review at least once each calendar year,[293] with certain exceptions, as described below.

Pursuant to Rule 1003(b)(1), ISE Internal Audit shall conduct an SCI Review of ISE's compliance with Regulation SCI not less than once each calendar year; provided, however, that:

- Rule 1003(b)(1)(i): Penetration test reviews of the network, firewalls, and production systems shall be conducted at a frequency of not less than once every three years; and

- Rule 1003(b)(1)(ii): Assessments of SCI Systems directly supporting market regulation or market surveillance shall be conducted at a frequency based upon the risk assessment conducted as part of the SCI Review, but in no case less than once every three years.

a) Penetration Test Reviews: Rule 1003(b)(1)(i)

Rule 1003(b)(1)(i), *Obligations related to systems changes; SCI review – SCI review*, requires penetration test reviews of ISE network, firewalls, and production systems to be conducted not less than once every three years. This rule does not apply to ISE development and test systems.[294] However, ISE Internal Audit may determine that, based on its risk assessment, it is appropriate and/or necessary to conduct

[290] See Adopting Release at p. 361.
[291] See Adopting Release at pp. 357-58.
[292] See Internal Audit Charter – Deutsche Börse Group policy statement (11 June 2015), Section 5, *Responsibility*.
[293] While the rule requires that an SCI Review be conducted "not less than once each calendar year," ISE may determine that it is appropriate to conduct an assessment of an SCI System more frequently, particularly for Critical SCI Systems. See Adopting Release at p. 537, FN 1085.
[294] See Adopting Release at p. 534, FN 1677.

penetration test reviews more frequently than once every three years.[295] Refer to the *Regulation SCI: Annual Review Program – Internal Audit Approach.*

As documented in the *ISE Standard: Corporate Physical Security*, ISE will perform penetration tests on a two year interval basis, or when any significant changes to facilities, policies, procedures, or security service providers have occurred. Additionally, with regard to hosted data centers who perform their own penetration tests, upon ISE's request (which shall be made annually), hosted data centers shall provide ISE with confirmation that physical security penetration testing is performed, including the date of the most recent penetration test.

Additionally, as documented in the *ISE Information Security Policy*, the Technical Compliance Checking policy covers penetration testing and vulnerability assessments which may be carried out by independent experts specifically contracted for this purpose. Such assessments are useful in detecting vulnerabilities in the system being tested as well as determining how effective the controls are in preventing unauthorized access due to these vulnerabilities.

b) Assessments of SCI Systems Directly Supporting Market Regulation or Market Surveillance: Rule 1003(b)(1)(ii)

ISE Internal Audit is required to determine the specific frequency with which to conduct assessments of SCI Systems directly supporting market regulation or market surveillance depending on the risk assessment conducted as part of the annual SCI Review, provided that these systems are assessed at least once every three years.[296]

3. SCI REVIEW REPORT

Upon the completion of the SCI Review, ISE Internal Audit is required to prepare a report (**SCI Review Report**) for review and submission to the Commission.

Pursuant to Rule 1003(b), *Obligations related to systems changes; SCI review – SCI review*, ISE shall:

- Rule 1003(b)(2): Submit a report of the SCI Review required by Rule 1003(b)(1) to senior management of ISE for review no more than 30 calendar days after completion of such SCI Review; and

- Rule 1003(b)(3): Submit to the Commission, and to the board of directors of ISE or the equivalent of such board, a report of the SCI Review required by Rule 1003(b)(1), together with any response by senior management, within 60 calendar days after its submission to senior management of ISE.

Because reports of SCI Reviews and any responses by senior management are required to be filed using Form SCI under the Exchange Act and Regulation SCI, it is unlawful for any person to willfully or knowingly

[295] See Adopting Release at p. 356.
[296] See Adopting Release at pp. 354-55.

make, or cause to be made, a false or misleading statement with respect to any material fact in such reports or responses.[297]

a) SCI Review Report – Senior Management Review: Rule 1003(b)(2)

ISE's senior management must receive the SCI Review Report from ISE Internal Audit no more than 30 calendar days after completion of an SCI Review.[298]

Rule 1003(b)(2), *Obligations related to systems changes; SCI review – SCI review*, promotes the responsibility and accountability of ISE senior management by helping to ensure that senior management:

- receives and reviews SCI Review Reports,
- is made aware of issues relating to compliance with Regulation SCI, and
- is encouraged to promptly establish plans for resolving such issues.[299]

Awareness by ISE's senior management of SCI Reviews and issues with Regulation SCI compliance should help to promote a focus by senior management on such reviews and issues, enhance communication and coordination regarding such reviews and issues among business, technology, legal, and compliance personnel and, in turn, strengthen the capacity, integrity, resiliency, and availability of SCI Systems.[300]

It is important that ISE's senior management receive and carefully review SCI Review Reports.[301] ISE senior management, after reviewing the SCI Review Report, should note, in addition to any other response that may be made, any material inaccuracy or omission that, to their knowledge, is in the report.[302]

(1) Definition of Senior Management

In the context of the SCI Review, senior management should not be limited to a single individual or officer of ISE.[303] Pursuant to Rule 1000, *Definitions*, senior management means, for purposes of Rule 1003(b), ISE's:

- Chief Executive Officer,
- Chief Technology Officer,
- Chief Information Officer,
- General Counsel, and
- Chief Compliance Officer,

or the equivalent of such employees or officers of ISE.

---

[297] See Adopting Release at p. 363.
[298] See Adopting Release at pp. 457-58.
[299] See Adopting Release at p. 363.
[300] See Adopting Release at p. 364.
[301] See Adopting Release at pp. 363-64.
[302] See Adopting Release at p. 360.
[303] See Adopting Release at p. 363.

These employees and officers, or their functional equivalent, represent the executive, technology, legal, and compliance functions that are necessary to effectively review the reports of SCI Reviews.[304]

Consistent with the requirements of Rule 1003(b)(2), *Obligations related to systems changes; SCI review – SCI review*, and the related definition in Rule 1000, *Definitions*, ISE has identified its Rule 1003(b)(2) senior management in **Appendix A: Senior Management – Rule 1003(b)(2)**.

b) SCI Review Report – Submission to the Commission & ISE Board of Directors: Rule 1003(b)(3)

Rule 1003(b)(3), *Obligations related to systems changes; SCI review – SCI review*, requires that ISE submit the SCI Review Report to ISE's Board of Directors and the Commission, together with any response by ISE senior management, within 60 calendar days after ISE Internal Audit's submission of the report to senior management.

Submission to ISE's Board of Directors. To help ensure that persons at the highest levels of ISE are made aware of any issues raised in the SCI Review, ISE Internal Audit is required to submit to ISE's Board of Directors, or the equivalent of such board, the SCI Review Report and any response by senior management within 60 calendar days after the submission of the SCI Review Report to ISE senior management.[305]

Submission to the Commission / Form SCI. The SCI Review Report must also be submitted to the Commission, via Form SCI, within 60 calendar days after the submission of the SCI Review Report to ISE senior management, and must include any response by ISE senior management to the report. Form SCI, along with Exhibit 5, *Report of SCI Review*, will be filed with the Commission by the ISE Compliance Officer or General Counsel.

Consistent with the requirements of Rule 1003(b)(2), ISE Internal Audit shall:

- Prepare a draft SCI Review Report upon conclusion of the SCI Review;
- Within 30 days after the completion of such SCI Review, submit the draft SCI Review Report to ISE senior management for review and comment;
- Maintain a copy of any senior management responses to the SCI Review Report;
- Within 60 calendar days after submission of the draft SCI Review Report to senior management, submit the final SCI Review Report, together with any response by senior management, to:
    - ISE's Board of Directors (or the equivalent of such board); and
    - The ISE Compliance Officer (with a copy to the General Counsel) who will file the final SCI Review Report, along with senior management responses, with the Commission on Form SCI.[306]

[304] See Adopting Release at p. 364.
[305] See Adopting Release at p. 364.
[306] To the extent the ISE Compliance Officer is unavailable, the General Counsel shall file the final SCI Review Report, along with senior management responses, with the Commission on Form SCI.

B. AUDIT OF THE EFFECTIVENESS OF RULE 1001 POLICIES AND PROCEDURES

Rules 1001(a)(3), (b)(3), and (c)(2) require periodic review by ISE of the effectiveness of its policies and procedures required by Rule 1001, *Obligations related to policies and procedures of SCI entities* and prompt action by ISE to remedy deficiencies in such policies and procedures.[307]

The Commission believes that requiring periodic review of the policies and procedures, and remedial actions to address any deficiencies in the policies and procedures, will help to ensure that ISE maintains robust policies and procedures and updates them when necessary so that the benefits of Rules 1001(a), (b), and (c) should continue to be realized.[308]

Diligence is required in maintaining a reasonable set of policies and procedures that keeps pace with changing technology and circumstances and does not become outdated over time.[309] While a systems problem may be probative as to the reasonableness of ISE's policies and procedures, it is not determinative.[310] Thus, the reasonably designed policies and procedures approach taken in Rule 1001(a) does not require ISE to guarantee flawless systems.[311]

ISE will not be found to be in violation of this maintenance requirement solely because it failed to identify a deficiency in its policies and procedures immediately after the deficiency occurred *if*:

- ISE takes prompt action to remedy the deficiency once it is discovered, and
- ISE had otherwise reviewed the effectiveness of its policies and procedures and took prompt action to remedy those deficiencies that were discovered, as required by Rule 1001(a)(3).[312]

1. CAPACITY, INTEGRITY, RESILIENCY, AVAILABILITY, AND SECURITY: RULE 1001(a)(3)

Rule 1001(a)(3), *Obligations related to policies and procedures of SCI entities – Capacity, integrity, resiliency, availability, and security*, requires that ISE shall periodically review the effectiveness of the policies and procedures required by Rules 1001(a)(2), and take prompt action to remedy deficiencies in such policies and procedures.[313]

In addition to the independent, periodic review of the effectiveness of ISE's Rule 1001(a)(2) policies and procedures by ISE Internal Audit or an external independent body, required to be performed on an annual basis, ISE management shall review and update its Rule 1001(a) policies and procedures **annually**, the timing of which shall be coordinated by management each year.

---

[307] See Adopting Release at pp. 153-54.
[308] See Adopting Release at p. 655.
[309] See Adopting Release at p. 153.
[310] See Adopting Release at p. 154.
[311] See Adopting Release at p. 153.
[312] See Adopting Release at p. 154.
[313] See Adopting Release at p. 451.

2. SYSTEMS COMPLIANCE: RULE 1001(b)(3)

Rule 1001(b)(3), *Obligations related to policies and procedures of SCI entities – Systems compliance*, requires that ISE shall periodically review the effectiveness of the policies and procedures required by Rule 1001(b)(2), and take prompt action to remedy deficiencies in such policies and procedures.[314]

In addition to the independent, periodic review of the effectiveness of ISE's Rule 1001(b)(2) policies and procedures by ISE Internal Audit or an external independent body, required to be performed on an annual basis, ISE management shall review and update its Rule 1001(b)(3) policies and procedures **annually**, the timing of which shall be coordinated by management each year.

3. RESPONSIBLE SCI PERSONNEL: RULE 1001(c)(2)

Rule 1001(c)(2), *Obligations related to policies and procedures of SCI entities – Responsible SCI personnel*, requires that ISE shall periodically review the effectiveness of the policies and procedures required by Rule 1001(c)(1), and take prompt action to remedy deficiencies in such policies and procedures.[315]

In addition to the independent, periodic review of the effectiveness of ISE's Rule 1001(c)(1) policies and procedures by ISE Internal Audit or an external independent body, required to be performed on an annual basis, ISE management shall review and update its Rule 1001(c)(1) policies and procedures **annually**, the timing of which shall be coordinated by management each year.

Consistent with the requirements of Rule 1003(b), *Obligations related to systems changes; SCI review – SCI review*, and in order to effectively perform the annual SCI Review in compliance with the requirements of Rule 1003(b), Rule 1001(a)(3), Rule 1001(b)(3) and Rule 1001(c)(2), discussed above, ISE Internal Audit has implemented and documented its annual SCI Review approach in the *Regulation SCI: Annual Review Program – Internal Audit Approach*.

INTENTIONALLY LEFT BLANK

[314] See Adopting Release at p. 452.
[315] See Adopting Release at p. 452.

X. BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN TESTING

Rule 1004, *SCI entity business continuity and disaster recovery plans testing requirements for members or participants*, requires ISE to mandate participation by designated members or participants in scheduled testing of the operation of its business continuity and disaster recovery plans, including backup systems, and to coordinate such testing on an industry- or sector-wide basis with other SCI Entities.[316]

Rule 1004 may require ISE to submit proposed rule changes, under Section 19(b) of the Exchange Act to the Commission for purposes of effectuating this requirement on its members. ISE's SCI SRO rulemaking authority would enable ISE to implement this requirement:

- SROs have the authority, and legal responsibility, under Section 6 of the Exchange Act, to adopt and enforce rules (including rules to comply with Regulation SCI's requirements relating to BC/DR testing) applicable to their members or participants that are designed to, among other things, foster cooperation and coordination with persons engaged in regulating, clearing, settling, processing information with respect to, and facilitating transactions in securities, to remove impediments to and perfect the mechanism of a free and open market and a national market system, and, in general, to protect investors and the public interest.[317]

Consistent with the requirements of Rule 1004, two Section 19(b) rule filings ("rule filings") were submitted to the Commission, the purpose of which are to amend: (i) ISE Rule 803, *Obligations of Market Makers*, to require Primary Market Makers, as Designated Members, to participate in functional and performance testing of the operation of ISE business continuity and disaster recovery plans at least once every 12 months; and (ii) ISE Rule 1903, *Order Routing to Other Exchanges*, to require Linkage Handlers, as Designated Members, to participate in functional and performance testing of the operation of ISE business continuity and disaster recovery plans at least once every 12 months. These rule filings are:

- **For ISE:** SR-ISE-2015-35 (October 23, 2015); and
- **For ISE Gemini:** SR-ISE Gemini-2015-23 (October 23, 2015).[318]

In particular, Rule 1004 requires that, with respect to ISE's business continuity and disaster recovery plans,[319] including its backup systems, ISE shall:

- Rule 1004(a): Establish standards for the designation of those members or participants that ISE reasonably determines are, taken as a whole, the minimum necessary for the maintenance of fair and orderly markets in the event of the activation of such plans;

---

[316] See Adopting Release at p. 2.

[317] See Adopting Release at pp. 378-79.

[318] **THIS SECTION WILL HAVE TO BE REVISED.** At the request of Business Development we will be changing the criteria for designating members to participate in BC/DR testing. A proposal will be submitted to the Board next week and then filed with the SEC. [Per Claire McG, 11-6-15]

[319] ISE's business continuity and disaster recovery plans are discussed in *Business Continuity and Disaster Recovery Plans: Rule 1001(a)(2)(v),* above.

- Rule 1004(b): Designate members or participants pursuant to the standards established in Rule 1004(a) and require participation by such designated members or participants in scheduled functional and performance testing of the operation of such plans, in the manner and frequency specified by ISE, provided that such frequency shall not be less than once every 12 months; and
- Rule 1004(c): Coordinate the testing of such plans on an industry- or sector-wide basis with other SCI Entities.

In the event of a wide-scale disruption in the securities markets, ISE and its members or participants may not be able to provide the same level of liquidity as on a normal trading day. The concept of "fair and orderly markets" does not require that trading on a day when business continuity and disaster recovery plans are in effect will reflect the same levels of liquidity, depth, volatility, and other characteristics of trading on a normal trading day.[320]

Nevertheless, the Commission believes it is critical that SCI Entities and their designated members or participants be able to operate with the SCI Entities' backup systems in the event of a wide-scale disruption. Therefore, Rule 1004 requires that ISE's BC/DR plan that meets the requirements of Rule 1001(a)(2)(v), *Obligations related to policies and procedures of SCI entities – Capacity, integrity, resiliency, availability, and security*, be tested for both its functionality and performance as specified by ISE's BC/DR plan.[321]

A. Designation Standards for Member BC/DR Testing: Rule 1004(a)

Rule 1004(a), *SCI entity business continuity and disaster recovery plans testing requirements for members or participants*, requires that ISE establish standards for the designation of those members or participants that ISE reasonably determines are, taken as a whole, the minimum necessary for the maintenance of fair and orderly markets in the event of the activation of such plans.

The requirement will help reduce the risks associated with ISE's decision to activate its BC/DR plans and help to ensure that such plans operate as intended, if activated.[322]

In developing its designation standards, ISE should "exercise reasonable judgment" in determining which of its members or participants collectively represent sufficient liquidity for ISE to maintain fair and orderly markets in a BC/DR scenario following a wide-scale disruption,[323] but should also be cautious that its designations are not overly limited.[324]

- The Commission believes that broad participation in BC/DR testing will enhance the utility of the testing, and that allowing non-designated members or participants the opportunity to participate in such testing generally will further this goal. Therefore, the Commission encourages SCI Entities

[320] See Adopting Release at p. 388. Further, Rule 1001(a)(2)(v), *Obligations related to policies and procedures of SCI entities – Capacity, integrity, resiliency, availability, and security*, does not require ISE to require members or participants to use the backup facility in the same way it uses the primary facility. See Adopting Release at p. 174.
[321] See Adopting Release at p. 388.
[322] See Adopting Release at p. 462.
[323] See Adopting Release at p. 376.
[324] See Adopting Release at pp. 376-77.

to permit non-designated members or participants to participate in the testing of the SCI Entity's BC/DR plans if they request to do so.[325]

ISE must keep records of its standards and designations.[326] ISE's standards, designations, and updates, if applicable, would be part of its records and therefore available to the Commission and its staff upon request,[327] for example, during its examination of ISE.[328]

The compliance date for ISE to set designation standards for members or participants to participate in scheduled functional and performance testing is November 3, 2015, as clarified by the Commission during the TCP 2015 Reg SCI Outreach.

Consistent with the requirements of Rule 1004(a), ISE has developed the following standards for designating ISE members for participation in its BC/DR testing.

1. ISE DESIGNATION STANDARDS FOR MEMBER BC/DR TESTING: RULE 1004(a)[329]

Pursuant to Rule 1004(a), ISE has established the following designation standards for member participation in functional and performance of testing of its BC/DR plans:

- All Primary Market Makers (**PMM**s); and
- *Select* Electronic Access Members (**EAM**s).
  - ISE has determined that only those EAMs that also serve as Linkage Handlers[330] will be designated for member BC/DR testing.

B. MEMBERS DESIGNATED FOR ISE BC/DR TESTING: RULE 1004(b)

Rule 1004(b), *SCI entity business continuity and disaster recovery plans testing requirements for members or participants*, requires ISE to designate members or participants pursuant to the standards established in Rule 1004(a) and require participation by such designated members or participants in scheduled functional and performance testing of the operation of such plans, in the manner and frequency specified by ISE, provided that such frequency shall not be less than once every 12 months.

The designation of a firm to participate in ISE's BC/DR testing means that such firm is significant, as ISE has reasonably determined it to be included in the set of its members or participants that is, "taken as a

---

[325] See Adopting Release at p. 377.
[326] See Adopting Release at p. 368.
[327] See Adopting Release at p. 377.
[328] See Adopting Release at pp. 377-78.
[329] **THIS SECTION WILL HAVE TO BE REVISED.** At the request of Business Development we will be changing the criteria for designating members to participate in BC/DR testing. A proposal will be submitted to the Board next week and then filed with the SEC. [Per Claire McG, 11-6-15]
[330] Established in 2013, Linkage Handers are EAMs that have entered into arrangements with ISE to provide routing broker services in accordance with ISE's rules and the Options Order Protection and Locked/Crossed Market Plan.

whole, the minimum necessary for the maintenance of fair and orderly markets in the event of the activation of such plans."[331]

The compliance date for ISE to designate members or participants to participate in scheduled functional and performance testing is November 3, 2015, as clarified by the Commission during the TCP 2015 Reg SCI Outreach.

Consistent with the requirement of Rule 1004(b) and ISE's designation standards pursuant to Rule 1004(a), above, ISE members designated to participate in the annual functional and performance testing of the operation of ISE's BC/DR plans are listed in **Appendix H: ISE Members Designated for Annual Functional and Performance Testing – Rule 1004(b)**. As a policy matter, ISE shall review (and update as necessary) this list at least annually, prior to the planned date of annual functional and performance testing of ISE's BC/DR plans, to ensure that the current list is complete.

C. FUNCTIONAL AND PERFORMANCE TESTING: RULE 1004(b)

Rule 1004(b) requires that ISE's BC/DR plan, pursuant to the requirements of Rule 1001(a)(2)(v), *Obligations related to policies and procedures of SCI entities – Capacity, integrity, resiliency, availability, and security*, be tested for both its functionality and performance, as specified by ISE's BC/DR plan.[332] Functional and performance testing of ISE's BC/DR plan shall be conducted with the designated members identified in *Members Designated for ISE BC/DR Testing: Rule 1004(b)*, above.

Functional Testing. Functional testing is commonly understood to examine whether a system operates in accordance with its specifications.[333]

Performance Testing. Performance testing examines whether a system is able to perform under a particular workload.[334] It should be noted that performance testing is not synonymous with "stress testing," in which capacity limits are tested.[335]

Rule 1004 provides ISE with discretion to determine the precise manner and content of the BC/DR testing required pursuant to Rule 1004, and ISE has discretion to determine, for example, the duration of the testing, the sample size of transactions tested, the scenarios tested, and the scope of the test.[336]

Commission Guidance for ISE to consider when planning and performing functional and performance testing includes:

- The testing frequency of once every 12 months is an appropriate minimum frequency that encourages regular and focused attention on the establishment of meaningful and effective testing. This requirement does not prevent ISE from testing more frequently, but rather is

[331] See Adopting Release at p. 381.
[332] See Adopting Release at p. 388.
[333] See Adopting Release at p. 383.
[334] See Adopting Release at p. 383.
[335] See Adopting Release at p. 387.
[336] See Adopting Release at p. 390.

intended to give ISE the flexibility to test its BC/DR plans, including its backup systems, at more frequent intervals if ISE finds it appropriate to do so.[337]

- The rule does not require ISE to test its BC/DR plan in live production, but also does not prohibit ISE from testing its BC/DR plans in live production, either, if ISE determines such a method of testing to be appropriate.[338]

- Functional and performance testing should include not only testing of connectivity, but also testing of ISE's systems, such as order entry, execution, clearance and settlement, order routing, and the transmission and/or receipt of market data, as applicable, to determine if they can operate as contemplated by ISE's business continuity and disaster recovery plans.[339]

- The Commission encourages ISE to develop one or more test scripts contemplating a wide-scale disruption and the enactment by SCI Entities in the region of the wide-scale disruption of their BC/DR plans.[340]

- While comments urging the creation of uniform test tickers, establishment of principles for end-to-end testing, mandatory types of test scripts, and cross-asset and cross-jurisdictional coordination are matters that ISE may wish to consider in implementing the testing required by the rule, the Commission does not believe it is appropriate to mandate such details in Regulation SCI, as this requirement is designed to provide SCI Entities flexibility and discretion in determining how to meet it.[341]

- The Commission has determined not to prescribe the time of day or week during which testing shall occur. The Commission continues to believe that SCI Entities are in the best position to structure the details of the test in a way that would maximize its utility.[342]

- The requirement to conduct "functional and performance testing of the operation of BC/DR plans" does not mean that a full test of the functional and performance characteristics of each backup facility is required to be conducted all at once and in coordination with other SCI Entities all at the same time.[343]

- Conducting the required testing is not intended to require market downtime, but permits a range of possibilities, as ISE determines to be appropriate, including weekend testing, as well as testing in segments over the course of a year, if ISE determines that, to meet the requirements of the rule, a single annual test cannot be properly conducted within a single period of time (*e.g.*, over the course of a weekend).[344]

---

[337] See Adopting Release at p. 392.
[338] See Adopting Release at p. 391.
[339] See Adopting Release at pp. 385-86.
[340] See Adopting Release at pp. 387-88.
[341] See Adopting Release at p. 390.
[342] See Adopting Release at p. 391.
[343] See Adopting Release at p. 386.
[344] See Adopting Release at p. 386, FN 1182.

- Nothing in Rule 1001(a) nor Rule 1004 requires that ISE's BC/DR plan specify that its backup site must fully replicate the capacity, speed, and other features of the primary site.[345]
- ISE's members and participants are not required by Regulation SCI to maintain the same level of connectivity with the backup sites of ISE as they do with the primary sites.[346]

- In the event of a wide-scale disruption in the securities markets, ISE and its members or participants may not be able to provide the same level of liquidity as on a normal trading day. The concept of "fair and orderly markets" does not require that trading on a day when business continuity and disaster recovery plans are in effect will reflect the same levels of liquidity, depth, volatility, and other characteristics of trading on a normal trading day. Nevertheless, it is critical that ISE and its designated members or participants be able to operate with ISE's backup systems in the event of a wide-scale disruption.[347]

- The **testing of BC/DR plans**, which is required by Rule 1004, is different from testing of the function and performance of backup facilities generally.[348] Testing of the function and performance of backup facilities generally would occur before such facilities are launched into production (such as pursuant to Rule 1001(a)), and Regulation SCI does not impose a requirement for coordinating such testing with other SCI Entities.[349] What Rule 1004 requires is coordinated testing to evaluate annually whether such backup facilities of SCI Entities can function and perform in accordance with the operation of BC/DR plans in the event of wide-scale disruption.[350]

The deadline for ISE to conduct initial Rule 1004(b) functional and performance testing of its BC/DR plan is November 2, 2016 (*i.e.*, within 12 months from the Regulation SCI November 3, 2015 **Compliance Date**).[351]

ISE maintains a *Business Continuity / Disaster Recovery Test Schedule*, updated annually, where it lists the tests planned for the current year**.**

D. INDUSTRY- OR SECTOR-WIDE TESTING OF BC/DR PLANS: RULE 1004(c)

Rule 1004(c), *Obligations related to policies and procedures of SCI entities – Capacity, integrity, resiliency, availability, and security*, requires ISE to coordinate such required testing on an industry- or sector-wide basis with other SCI entities.

As clarified in the Regulation SCI FAQs, Rule 1004 does not require two separate tests of BC/DR plans. Instead, SCI Entities can conduct functional and performance testing of BC/DR plans with the

[345] See Adopting Release at p. 388.
[346] See Adopting Release at p. 388.
[347] See Adopting Release at p. 388.
[348] See Adopting Release at p. 386.
[349] See Adopting Release at p. 386, FN 1183.
[350] See Adopting Release at pp. 386-87.
[351] See Regulation SCI FAQs at: http://www.sec.gov/divisions/marketreg/regulation-sci-faq.shtml

participation of designated members or participants, and in coordination with other SCI Entities on an industry- or sector-wide basis, not less than once every 12 months.[352]

The Commission believes that it would be more cost-effective for SCI Entity members and participants to participate in testing of SCI Entity BC/DR plans on an industry- or sector-wide basis than to test with each SCI Entity on an individual basis because such coordination would likely reduce duplicative testing efforts.[353] Because, coordinating industry- or sector-wide testing among SCI Entities and their designated members or participants may present logistical challenges, the coordination requirement provides discretion to SCI Entities to determine how to meet it.[354]

The Industry- Sector-Wide BC/DR Testing Compliance Date for conducting industry- or sector-wide testing of BC/DR plans is November 2, 2017, as clarified by the Commission during the TCP 2015 Reg SCI Outreach as well as in the Regulation SCI FAQs.

Consistent with the requirements of Rule 1004(c), ISE currently participates in an industry testing working group, the purpose of which is to devise an industry- or sector-wide BC/DR testing plan.

When the industry-wide testing plan by the industry working group has been finalized, this section will be updated.

INTENTIONALLY LEFT BLANK

[352] See Regulation SCI FAQs.
[353] See Adopting Release at p. 395.
[354] See Adopting Release at p. 394.

XI. RECORDKEEPING REQUIREMENTS

A. ONGOING RECORDKEEPING REQUIREMENTS: RULE 1005(a)

Rule 1005, *Recordkeeping requirements related to compliance with Regulation SCI*, sets forth recordkeeping requirements for SCI Entities. Applicable to ISE, as an SCI SRO, are Rules 1005(a) and 1005(c). Rule 1005(b) applies to SCI Entities that are not SCI SROs. With respect to SCI SROs in particular, the Commission notes that they are subject to the recordkeeping requirements of Rule 17a-1 under the Exchange Act, and the breadth of Rule 17a-1 is such that it would require SCI SROs to make, keep, and preserve records relating to their compliance with Regulation SCI.[355]

Pursuant to Rule 1005(a), *Recordkeeping requirements related to compliance with Regulation SCI*, ISE shall make, keep, and preserve all documents relating to its compliance with Regulation SCI as prescribed in §240.17a-1[356] of the Securities Exchange Act.

Consistent with the requirements of Regulation SCI Rule 1005(a) and Securities Exchange Act Rule 17a-1, ISE maintains a *Record Retention Policy* which is documented in the *ISE Code of Business Conduct and Ethics*.

B. RECORDKEEPING REQUIREMENTS IN THE EVENT OF CLOSURE: RULE 1005(c)

Pursuant to Rule 1005(c), *Recordkeeping requirements related to compliance with Regulation SCI*, upon or immediately prior to ceasing to do business or ceasing to be registered under the Securities Exchange Act of 1934, ISE shall take all necessary action to ensure that the records required to be made, kept, and preserved by Rule 1005 shall be accessible to the Commission and its representatives in the manner required by Rule 1005 and for the remainder of the period required by Rule 1005.

Consistent with the requirements of Rule 1005(c), ISE maintains a *Record Retention Policy* which is documented in the *ISE Code of Business Conduct and Ethics***.**

C. REQUIREMENTS FOR SERVICE BUREAUS: RULE 1007

The purpose of Rule 1007, *Requirements for service bureaus*, is to ensure the Commission's ability to obtain required records that are held by a third party who may not otherwise have an obligation to make such records available to the Commission.[357]

Under Rule 1007, *Requirements for service bureaus*, if records required to be filed or kept by ISE under Regulation SCI are prepared or maintained by a service bureau or other recordkeeping service on behalf

---

[355] See Adopting Release at p. 699.
[356] 17 CFR 240.17a-1, *Recordkeeping rule for national securities exchanges, national securities associations, registered clearing agencies and the Municipal Securities Rulemaking Board*.
[357] See Adopting Release at pp. 403-04.

of ISE, ISE shall ensure that the records are available for review by the Commission and its representatives by submitting a **written undertaking**, in a form acceptable to the Commission, by such service bureau or other recordkeeping service, signed by a duly authorized person at such service bureau or other recordkeeping service.

1. WRITTEN UNDERTAKING BY SERVICE BUREAU OR OTHER RECORDKEEPING SERVICE: RULE 1007

The purpose of the written undertaking is to ensure that a service bureau or other recordkeeping service is aware of its obligation with respect to records relating to Regulation SCI and ensure that the Commission has prompt and efficient access to all required records, including those housed at a service bureau or any other recordkeeping service.[358]

In this regard, Rule 1007, *Requirements for service bureaus*, further states that such a written undertaking shall include an agreement by the service bureau to permit the Commission and its representatives to examine such records at any time or from time to time during business hours, and to promptly furnish to the Commission and its representatives true, correct, and current electronic files in a form acceptable to the Commission or its representatives or hard copies of any or all or any part of such records, upon request, periodically, or continuously and, in any case, within the same time periods as would apply to ISE for such records.

2. SCI ENTITY RECORDKEEPING OBLIGATIONS REMAIN UNCHANGED: RULE 1007

Additionally, under Rule 1007, *Requirements for service bureaus*, the preparation or maintenance of records by a service bureau or other recordkeeping service shall not relieve ISE from its obligation to prepare, maintain, and provide the Commission and its representatives access to such records.

Currently, ISE does not have any relationships with service bureaus.

INTENTIONALLY LEFT BLANK

[358] See Adopting Release at p. 404.

XII. ELECTRONIC FILING AND SUBMISSION (*Form SCI*)

Rule 1006, *Electronic filing and submission*, is intended to provide a uniform manner in which the Commission would receive—and SCI Entities would provide—written notifications, reviews, descriptions, analyses, or reports made pursuant to Regulation SCI.

With certain exceptions, ISE is required to file all notifications or submissions to the Commission via Form SCI under Rule 1006, *Electronic filing and submission*.

In particular, Rule 1006(a), *Electronic filing and submission*, states: Except with respect to notifications to the Commission pursuant to Rule 1002(b)(1)[359] or updates to the Commission made pursuant to Rule 1002(b)(3),[360] any notification, review, description, analysis or report to the Commission required to be submitted under Regulation SCI shall be filed electronically on Form SCI,[361] include all information as prescribed in Form SCI and the instructions thereto,[362] and contain an electronic signature.[363]

A. CONFIDENTIAL TREATMENT OF FORM SCI FILINGS – EXCHANGE ACT RULE 24b-2g

To permit implementation of Rule 1006, the Commission is adopting an amendment to Rule 24b-2 under the Exchange Act.[364] Under Rule 24b-2 of the Exchange Act, new paragraph (g) will provide that an SCI Entity's electronic filings on Form SCI pursuant to Regulation SCI must include any information with respect to which confidential treatment is requested ("confidential portion"), and provides that, in lieu of the procedures described in Rule 24b-2b, an SCI Entity may request confidential treatment of all information submitted on Form SCI by completing Section IV, *Signature*, of Form SCI.

- The Commission's amendment provides an exception from Rule 24b-2's paper-only request for confidential treatment for all Form SCI filings, and specifically permits an SCI Entity to electronically request confidential treatment of all information filed on Form SCI in accordance with Regulation SCI.

Provided the confidential treatment request is properly made, electronic submission of confidential treatment requests will expedite Commission review of the requests for confidential treatment, as all information submitted on Form SCI will be deemed to be the subject of the request for confidential treatment.

If such a confidential treatment request is properly made, the Commission will keep the information collected pursuant to Form SCI confidential to the extent permitted by law.[365]

---

[359] Covers immediate Commission notification regarding SCI Events.
[360] Covers regular Commission updates regarding SCI Events.
[361] See **Appendix J-1: Form SCI**, for a copy of Form SCI.
[362] See **Appendix J-3: Form SCI – General Instructions**, for the instructions to Form SCI.
[363] See *Electronic Signature: Rule 1006(b) and Rule 1000*, below, for details.
[364] 17 CFR 240.24b-2. *Nondisclosure of information filed with the Commission and with any Exchange*.
[365] See Adopting Release at pp. 408-409.

1. THE FREEDOM OF INFORMATION ACT ("FOIA")

The Freedom of Information Act ("FOIA") provides at least two pertinent exemptions under which the Commission has authority to withhold certain information:

- FOIA Exemption 4 provides an exemption for "trade secrets and commercial or financial information obtained from a person and privileged or confidential." 5 U.S.C. 552(b)(4).

- FOIA Exemption 8 provides an exemption for matters that are "contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions." 5 U.S.C. 552(b)(8).[366]

The information submitted to the Commission pursuant to Rule 1006, *Electronic filing and submission*, that is filed on Form SCI, will be treated as confidential, subject to applicable law, including amended Rule 24b-2.[367]

B. FORM SCI – §249.1900

Rule 1006 provides that, except with respect to notifications to the Commission made pursuant to Rule 1002(b)(1),[368] or updates to the Commission made pursuant to Rule 1002(b)(3),[369] any all notification, review, description, analysis, or report to the Commission required to be submitted under Regulation SCI shall be filed electronically on Form SCI, include all information as prescribed in Form SCI and the instructions thereto, and contain an electronic signature.

An example of Form SCI is contained in **Appendix J-1: Form SCI**. The instructions to Form SCI is contained in **Appendix J-3: Form SCI – General Instructions**.

1. FORM SCI SCHEDULE OF EXHIBITS

Form SCI is required to be filed with exhibit(s) attached that fall into one of six (6) categories of SCI filings:

- **Exhibit 1:** Rule 1002(b)(2) Notification of an SCI Event.
- **Exhibit 2:** Rule 1002(b)(4) Final or Interim Report of SCI Event
- **Exhibit 3:** Rule 1002(b)(5)(ii) Quarterly Report of de minimis SCI Events
- **Exhibit 4:** Quarterly Report of Systems Changes
- **Exhibit 5:** Rule 1003(b)(3) Report of SCI Review

---

[366] See Adopting Release at p. 409, FN 1247.
[367] See Adopting Release at p. 555.
[368] The initial, immediate notification to the Commission of the occurrence of an SCI Event, as described in *Initial Immediate Notification (Oral or Written): Rule 1002(b)(1)*, above.
[369] Regular updates to the Commission concerning the status of the SCI Event, as described in *Regular Updates to Commission: Rule 1002(b)(3)*, above.

- **Exhibit 6:** Optional Attachments

Refer to **Appendix J-2: Form SCI – Schedule of Exhibits**, for detailed explanation of these exhibits. Additionally, templates for Form SCI Exhibits 1 – 5 are stored on the Compliance Department's shared drive in the "Templates" sub-folder. They are also available to ISE Staff on the **J Drive** in the **Regulation SCI** folder / "**Toolkit**" sub-folder**.**

2. COMPLETING FORM SCI

When completing Form SCI, ISE must indicate on the form the specific type of submission it is making. That is, whether the submission is:

- a notification regarding an SCI Event pursuant to Rule 1002(b)(2);
- a final report or interim status report regarding an SCI Event pursuant to Rule 1002(b)(4);
- a quarterly report on de minimis Systems Disruptions and de minimis Systems Intrusions pursuant to Rule 1002(b)(5)(ii);
- a quarterly report of material systems changes pursuant to Rule 1003(a)(1);
- a supplemental report of material system changes pursuant to Rule 1003(a)(2); or
- a submission of the report of an SCI Review, together with any response by senior management, pursuant to Rule 1003(b)(3).[370]

For complete instructions on completing Form SCI, refer to **Appendix J-3: Form SCI – General Instructions**.

C. ELECTRONIC SIGNATURE: RULE 1006(b) AND RULE 1000

Pursuant to Rule 1006(b), *Electronic filing and submission*, the signatory to an electronically filed Form SCI shall manually sign a signature page or document, in the manner prescribed by Form SCI, authenticating, acknowledging, or otherwise adopting his or her signature that appears in typed form within the electronic filing.

The purpose of the electronic signature requirement on Form SCI is to ensure that the person submitting the form to the Commission has been properly authorized by ISE to submit the form on its behalf,[371] thereby helping ensure the authenticity of the Form SCI submission.[372]

Pursuant to Rule 1000, *Definitions*, electronic signature has the meaning set forth in §240.19b-4(j)[373] of this chapter:

- **240.19b-4 (j):** Filings by a self-regulatory organization submitted on Form 19b-4 (17 CFR 249.819) electronically shall contain an electronic signature. For the purposes of this section, the term *electronic signature* means an electronic entry in the form of a magnetic impulse or other form of computer data compilation of any letter or series of letters or characters comprising a

[370] See Adopting Release at p. 416.
[371] See Adopting Release at p. 407.
[372] See Adopting Release at p. 429.
[373] 17 CFR 240.19b-4, *Filings with respect to proposed rule changes by self-regulatory organizations.*

name, executed, adopted or authorized as a signature. The signatory to an electronically submitted rule filing shall manually sign a signature page or other document, in the manner prescribed by Form 19b-4, authenticating, acknowledging or otherwise adopting his or her signature that appears in typed form within the electronic filing. Such document shall be executed before or at the time the rule filing is electronically submitted and shall be retained by the filer in accordance with § 240.17a-1.

Similar to use of the EFFS[374] in the context of electronic filing of Form 19b-4, by using a digital ID for each duly authorized signatory providing an electronic signature, both the Commission and ISE may be assured of the authenticity and integrity of the electronic filing of Form SCI.

Thus, ISE will be required to have the ability to electronically submit Form SCI through the EFFS system, and every person designated to sign Form SCI will be required to have an electronic signature and a digital ID**.**

The electronic signature requirement would not put ISE personnel at risk if ISE later determines that there were factual errors, omissions, or other flaws in the initial filing.[375]

D. ISE AUTHORIZED FORM SCI PERSONNEL

Pursuant to the requirements of Rule 1006(b), ISE has designated the following Authorized Form SCI Personnel as ISE's official signatories to an electronically filed Form SCI, and has also made provisions to maintain the manual signature pages of such Authorized Form SCI Personnel.

Title	Current Title Holder Name	Manual signature on file/Location
Compliance Officer	Claire McGrath	Legal Department Files
General Counsel	Michael Simon	Legal Department Files

INTENTIONALLY LEFT BLANK

[374] The Electronic Form 19b-4 Filing System ("EFFS"), is a secure website operated by the Commission.
[375] See Adopting Release at p. 407.

XIII. SERVICE BUREAUS

As discussed in *Recordkeeping Requirements*, above, Rule 1007, *Requirements for service bureaus*, is a recordkeeping rule put in place to ensure that, if records required to be filed or kept by ISE under Regulation SCI are prepared or maintained by a service bureau or other recordkeeping service on behalf of ISE, ISE is required to ensure that the records prepared by the service bureau or other recordkeeping service are available for review by the Commission and its representatives by submitting a written undertaking, in a form acceptable to the Commission, by such service bureau or other recordkeeping service, signed by a duly authorized person at such service bureau or other recordkeeping service.

A. IDENTIFICATION OF SERVICE BUREAUS OR OTHER RECORDKEEPING SERVICES

Currently, ISE does not utilize service bureaus or other recordkeeping services. However, ISE must assess new third party relationships to determine whether such third party would be classified as a service bureau or other recordkeeping service under Regulation SCI.

When ISE determines that it is utilizing the services of a service bureau or other recordkeeping service, Rule 1007 requires ISE to establish a written undertaking with such service bureau or other recordkeeping service and submit same to the Commission. This requirement helps ensure that such service bureau or other recordkeeping service is aware of its obligations with respect to records relating to Regulation SCI.[376]

Such written undertaken shall be drafted by the ISE Legal Department, if the need arises.

B. WRITTEN UNDERTAKING BY SERVICE BUREAU OR OTHER RECORDKEEPING SERVICE

Consistent with the requirements of Rule 1007, and where applicable, all written undertakings between ISE and any service bureau or other recordkeeping service that prepares, on behalf of ISE, records required to be filed or kept by ISE under Regulation SCI shall be drafted by the ISE Legal Department and shall contain, at a minimum, the following provisions, as required by Regulation SCI:

- An agreement by the service bureau or other recordkeeping service to permit the Commission and its representatives to examine such records at any time or from time to time during business hours; and
- An agreement by the service bureau or other recordkeeping service to promptly furnish to the Commission and its representatives true, correct, and current electronic files in a form acceptable to the Commission or its representatives or hard copies of any or all or any part of such records, upon request, periodically, continuously and, in any case, within the same time periods as would apply to ISE for such records.[377]

[376] See Adopting Release at p. 404.
[377] Rule 1007, *Requirements for service bureaus.*

Such written undertaking must be signed by a duly authorized person at the service bureau or other recordkeeping service.

Submission of Written Undertaking to the Commission. The written undertaking may be in the form of a letter containing the required elements and should be submitted to the Commission as soon as ISE engages a service bureau or other recordkeeping service.[378] Commission Staff has further indicated that the written undertaking letter, as well as any subsequent update (as necessary), should be submitted either via email or physical mail[379] as follows:

Notification	Commission Contact
Emailed Submission	**cyberwatch@sec.gov**[380]
Physical Submission	INSERT DESIGNATED PHYSICAL ADDRESS FROM SEC WHEN RECEIVED

Confidential Requests. For any emailed submissions, ISE must make a confidential treatment request in paper format only,[381] pursuant to Rule 24b-2 under the Exchange Act.[382]

INTENTIONALLY LEFT BLANK

[378] See Regulation SCI FAQs at: http://www.sec.gov/divisions/marketreg/regulation-sci-faq.shtml
[379] See Regulation SCI FAQs.
[380] As advised by Commission Staff during the **Cyber Watch Call** between ISE and Commission Cyber Watch Team on October 27, 2015.
[381] See Adopting Release at p. 408
[382] See 17 CFR 240.24b-2.

THIS PAGE IS INTENTIONALLY BLANK

XIV. APPENDICES – TABLE OF CONTENTS

APPENDIX	DESCRIPTION
Appendix A	Senior Management – Rule 1003(b)(2)
Appendix B	Responsible SCI Personnel – Rule 1001(c)(1)
Appendix B-1	Responsible SCI Personnel Designees
Appendix C	SCI Systems
Appendix D	Critical SCI Systems
Appendix E	Indirect SCI Systems
Appendix F-1	THIRD PARTY – FINRA Regulation SCI Policies and Procedures
Appendix F-2	THIRD PARTY – Exegy Regulation SCI Policies and Procedures Pursuant to ISE *Policy: Third Party Providers of SCI Systems – Exegy*
Appendix G	Current SCI Industry Standards Mapping
Appendix H	ISE Members Designated for Annual Functional and Performance Testing
Appendix I	Regulation SCI Rules 1000 – 1007
Appendix J-1	Form SCI
Appendix J-2	Form SCI – Schedule of Exhibits
Appendix J-3	Form SCI – General Instructions

APPENDIX A: SENIOR MANAGEMENT – Rule 1003(b)(2)

Rule 1003(b)(2), *SCI Review*, requires that the report of any SCI Review be submitted to ISE senior management for review no more than 30 calendar days after completion of the review (**SCI Review Report**).

Below are the ISE senior management who must be provided a copy of the SCI Review Report pursuant to the requirements of Rule 1003(b)(2), *SCI Review*.

TITLE	NAME	PHONE	EMAIL
Chief Executive Officer	Gary Katz	(212) 897-0240	gkatz@ise.com
Chief Technology Officer	Robert J. Cornish	(212) 897-0258	rcornish@ise.com
Chief Information Officer	Daniel P. Friel	(212) 897-0260	dfriel@ise.com
General Counsel	Michael J. Simon	(212) 897-0230	msimon@ise.com
Compliance Officer	Claire McGrath	(212) 897-8130	cmcgrath@ise.com

APPENDIX B: RESPONSIBLE SCI PERSONNEL – Rule 1001(c)(1)

SCI SYSTEM	CATEGORY OF SCI SYSTEM (*SCI System; Critical SCI System; or Indirect SCI System*)	RESPONSIBLE SCI PERSONNEL[383] BY SCI EVENT		
		SYSTEM DISRUPTION	SYSTEM INTRUSION	SYSTEM COMPLIANCE ISSUE
TRADING				
Config Client	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
Exegy*	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
Exegy Feed Interface (EFI)	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
Index Feed Systems (IDS)	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
Market Place Tool (MPT) *Has Mkt Reg elements*	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
Market Watch (MW) *Has Mkt Reg elements*	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
Market Wide Speed Bump (MWSB) *Has Mkt Reg elements*	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
Matching Engine (ME)	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
OCC Trade Reporter (OCCTR)	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
OpCon	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
Orderbook Explorer (OBE)	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
PostProcessor (POPE)	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
Reference Data (Core)	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
Reference Data Cache External (RDCX)	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
Session Manager	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
System Controller (BOS)	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
System Monitor	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
Trade Manager (TM)	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
ORDER ROUTING				
Gateway / Outbound Feed Interface (GWY/OFI)	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
ISE Order Routing System (IORS)	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky

[383] See **Appendix B-1: Responsible SCI Personnel Designees**, for the list of ISE's RSP designees.

SCI SYSTEM	CATEGORY OF SCI SYSTEM (*SCI System; Critical SCI System; or Indirect SCI System*)	RESPONSIBLE SCI PERSONNEL[383] BY SCI EVENT		
		SYSTEM DISRUPTION	SYSTEM INTRUSION	SYSTEM COMPLIANCE ISSUE
Linkage Order Router (LOR)	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
PrecISE	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
Smart Order Router (SOR)	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
MARKET DATA				
Market Data Disseminator (MDD)	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
OPRA Quote/Tape Reporter (OQTR)	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
Reference Data Disseminator (RDD)	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
MARKET REGULATION				
Exegy Bridge Service (EBS)	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
Market Place Tool (MPT) – **(Duplicate)**	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
Market Watch (MW) – **(Duplicate)**	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
Market Wide Speed Bump (MWSB) – **(Duplicate)**	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
Real Time Processor (RTP)	SCI System	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky	Danny Friel Boris Ilyevsky
MARKET SURVEILLANCE				
Audit Trail Server	SCI System	Danny Friel Mike Simon	Danny Friel Mike Simon	Danny Friel Mike Simon
FINRA*	SCI System	Mike Simon	Mike Simon	Mike Simon
Surveillance	SCI System	Danny Friel Mike Simon	Danny Friel Mike Simon	Danny Friel Mike Simon

KEY: * - Third Party System

INDIRECT SCI SYSTEM / CATEGORY OF INDIRECT SCI SYSTEM	RESPONSIBLE SCI PERSONNEL SYSTEM INTRUSION[384]
See Appendix E, *Indirect SCI Systems*, below for examples of reporting categories for ISE Indirect SCI Systems.	Danny Friel Boris Ilyevsky

RESPONSIBLE SCI PERSONNEL CONTACT INFORMATION			
RESPONSIBLE SCI PERSONNEL	**TITLE**	**PHONE**	**EMAIL**
Daniel ("Danny") Friel	Chief Information Officer	212-897-0260	DFriel@ise.com
Boris Ilyevsky	Managing Director, ISE Options Exchange	212-897-0242	BIlyevsky@ise.com
Michael ("Mike") Simon	General Counsel, Chief Regulatory Officer & Secretary	212-897-0230	MSimon@ise.com

[384] Indirect SCI Systems are only subject to SCI Events that are Systems Intrusions. See Rule 1000, *Definitions*.

APPENDIX B-1: RESPONSIBLE SCI PERSONNEL DESIGNEES

SCI SYSTEM	CATEGORY OF SCI SYSTEM (*SCI System; Critical SCI System; or Indirect SCI System*)	DESIGNEES OF ISE RESPONSIBLE SCI PERSONNEL BY SCI EVENT		
		SYSTEM DISRUPTION	SYSTEM INTRUSION	SYSTEM COMPLIANCE ISSUE
TRADING				
Config Client	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
Exegy*	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
Exegy Feed Interface (EFI)	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
Index Feed systems (IDS)	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
Market Place Tool (MPT) *Has Mkt Reg elements*	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
Market Watch (MW) *Has Mkt Reg elements*	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
Market Wide Speed Bump (MWSB) *Has Mkt Reg elements*	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
Matching Engine (ME)	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
OCC Trade Reporter (OCCTR)	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
OpCon	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
Orderbook Explorer (OBE)	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
Post Processor (POPE)	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
Reference Data (Core)	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
Reference Data Cache External (RDCX)	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
Session Manager	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
System Controller (BOS)	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
System Monitor	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
Trade Manager (TM)	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
ORDER ROUTING				
Gateway / Outbound Feed Interface (GWY/OFI)	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
IORS	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
Linkage Order Router (LOR)	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
PrecISE	SCI System	Rob Cornish	Rob Cornish	Tom Reina

SCI SYSTEM	CATEGORY OF SCI SYSTEM (*SCI System; Critical SCI System; or Indirect SCI System*)	DESIGNEES OF ISE RESPONSIBLE SCI PERSONNEL BY SCI EVENT		
		SYSTEM DISRUPTION	**SYSTEM INTRUSION**	**SYSTEM COMPLIANCE ISSUE**
		Dan Amar	Dan Amar	Jeanine Hightower
Smart Order Router (SOR)	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
MARKET DATA				
Market Data Disseminator (MDD)	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
OPRA Quote/Tape Reporter (OQTR)	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
Reference Data Disseminator (RDD)	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
MARKET REGULATION				
Exegy Bridge Service (EBS)	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
Market Place Tool (MPT) – **(Duplicate)**	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
Market Watch (MW) _ **(Duplicate)**	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
Market Wide Speed Bump (MWSB) – **(Duplicate)**	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
Real Time Processor (RTP)	SCI System	Rob Cornish Dan Amar	Rob Cornish Dan Amar	Tom Reina Jeanine Hightower
MARKET SURVEILLANCE				
Audit Trail Server	SCI System	Rob Cornish Russ Davidson	Rob Cornish Russ Davidson	Tom Reina Russ Davidson
FINRA*	SCI System	Russ Davidson	Russ Davidson	Russ Davidson
Surveillance	SCI System	Rob Cornish Russ Davidson	Rob Cornish Russ Davidson	Tom Reina Russ Davidson

KEY: * - Third Party System

INDIRECT SCI SYSTEM / CATEGORY OF INDIRECT SCI SYSTEM	DESIGNEES OF RESPONSIBLE SCI PERSONNEL
	SYSTEM INTRUSION[385]
See Appendix E, *Indirect SCI Systems*, below for examples of reporting categories for ISE Indirect SCI Systems.	Rob Cornish Dan Amar

RESPONSIBLE SCI PERSONNEL DESIGNEE CONTACT INFORMATION			
RESPONSIBLE SCI PERSONNEL	**TITLE**	**PHONE**	**EMAIL**
Daniel ("Dan") Amar	Head of Market Operations	212-897-8146	damar@ise.com
Robert (Rob) Cornish	Chief Technology Officer	212-897-0258	rcornish@ise.com
Russ Davidson	Surveillance Officer	646-805-1857	rdavidson@ise.com
Jeanine Hightower	Business Development Officer	212-897-0357	jhightower@ise.com
Thomas ("Tom") Reina	Development Officer	212-897-8164	treina@ise.com

[385] Indirect SCI Systems are only subject to SCI Events that are Systems Intrusions. See Rule 1000, *Definitions*.

APPENDIX C: SCI SYSTEMS

Rule 1000, *Definitions*, defines an SCI System as all computer, network, electronic, technical, automated, or similar systems of, or operated by or on behalf of, ISE that, with respect to securities, directly support trading, clearance and settlement, order routing, market data, market regulation, or market surveillance.

Below are ISE's systems that are captured by the Rule 1000 definition of SCI System.

ISE SCI SYSTEM (*In Alphabetical Order*)	**ISE SYSTEM CATEGORY**	**REGULATION SCI SYSTEM CATEGORY** (*Trading; Clearance and Settlement; Order Routing; Market Data; Market Regulation; Market Surveillance*)
Audit Trail Server	Core	Market Surveillance
Config Client	ISE APPs	Trading
Exegy	**Third Party System**	Trading
Exegy Bridge Service (EBS)	ISE APPs	Market Regulation
Exegy Feed Interface (EFI)	Core	Trading
FINRA	**Third Party System**	Market Surveillance
Gateway / Outbound Feed Interface (GWY/OFI)	Core	Order Routing
Index Feed Systems (IDS)	ISE APPs	Trading
ISE Order Routing System (IORS)	ISE APPs	Order Routing
Linkage Order Router (LOR)	ISE APPs	Order Routing
Market Data Disseminator (MDD)	Core	Market Data
Market Place Tool (MPT)	ISE APPs	Trading
Market Place Tool (MPT) – **(Duplicate)**	ISE APPs	Market Regulation
Market Watch (MW)	ISE APPs	Trading
Market Watch (MW) – **(Duplicate)**	ISE APPs	Market Regulation
Market Wide Speed Bump (MWSB)	ISE APPs	Trading
Market Wide Speed Bump (MWSB) – **(Duplicate)**	ISE APPs	Market Regulation
Matching Engine (ME)	Core	Trading
OCC Trade Reporter (OCCTR)	ISE APPs	Trading
OpCon	Core	Trading
OPRA Quote/Tape Reporter (OQTR)	ISE APPs	Market Data

ISE SCI SYSTEM (*In Alphabetical Order*)	**ISE SYSTEM CATEGORY**	**REGULATION SCI SYSTEM CATEGORY** (*Trading; Clearance and Settlement; Order Routing; Market Data; Market Regulation; Market Surveillance*)
Orderbook Explorer (OBE)	ISE APPs	Trading
PostProcessor (POPE)	Core	Trading
PrecISE	ISE APPs	Order Routing
Real Time Processor (RTP)	ISE APPs	Market Regulation
Reference Data – (Core)	ISE APPs	Trading
Reference Data Cache External (RDCX)	ISE APPs	Trading
Reference Data Disseminator (RDD)	Core	Market Data
Session Manager	Core	Trading
Smart Order Router (SOR)	ISE APPs	Order Routing
Surveillance	ISE APPs	Market Surveillance
System Controller (BOS)	Core	Trading
System Monitor	Core	Trading
Trade Manager (TM)	Core	Trading

APPENDIX D: CRITICAL SCI SYSTEMS

Rule 1000, *Definitions*, defines a Critical SCI System as any SCI System of, or operated by or on behalf of, ISE that:

1) Directly support functionality relating to:
   (i) Clearance and settlement systems of clearing agencies;[386]
   (ii) Openings, reopenings, and closings on the primary listing market;[387]
   (iii) Trading halts;[388]
   (iv) Initial public offerings;[389]
   (v) The provision of consolidated market data;[390] or
   (vi) Exclusively-listed securities; or
2) Provide functionality to the securities markets for which the availability of alternatives is significantly limited or nonexistent and without which there would be a material impact on fair and orderly markets.

Since neither "exclusively listed securities" and FCOs are "systems," ISE interprets all SCI Systems[391] directly supporting the trading of FCOs as Critical SCI Systems.

REGULATION SCI CRITERA	PRODUCT DESCRIPTION	CRITICAL SCI SYSTEM
Exclusively-listed securities	ISE cash-settled, rate-modified foreign currency options (**FCOs**)	All SCI Systems directly supporting the trading of ISE FCOs

[386] Not applicable. ISE is not a clearing agency.
[387] Not applicable. ISE is not a primary listing market.
[388] Not applicable. See *Trading Halts: No Related ISE Critical SCI Systems*, above, for details.
[389] Not applicable. ISE is an options exchange and, therefore, does not issue initial public offerings (IPOs).
[390] Not applicable. ISE is not a securities information processor (SIP).
[391] See **Appendix C, *SCI Systems***, above, for the list of ISE SCI Systems.

APPENDIX E: INDIRECT SCI SYSTEMS[392]

Rule 1000, *Definitions*, defines Indirect SCI Systems as any systems of, or operated by or on behalf of, ISE that, if breached, would be reasonably likely to pose a security threat to ISE SCI Systems (see list of ISE SCI Systems at Appendix C, *SCI Systems*, above).

As documented in the *Standard – Indirect SCI Systems*, below are examples of reporting categories for ISE Indirect SCI Systems. These supporting systems are subject to change and therefore this section provides examples and guidance on categorization.

Exploratory services, such as proof-of-concept or beta systems, would not be subject to classification as Indirect SCI Systems, if adequately separated from SCI Systems.

APPLICATION FUNCTION	INDIRECT SCI SYSTEM CATEGORY	DIRECT CONNECTION TO SCI SYSTEM?	ASSAILABLE PROTOCOL[393]
Authentication and Authorization (Active Directory)	Cybersecurity controls	Yes	Yes
Anti-malware (McAfee)	Cybersecurity controls	Yes	Yes
Patch and Vulnerability Management (Nessus / Shavlik)	Cybersecurity controls	Yes	Yes
Security Information and Event Monitoring (SIEM)	Cybersecurity controls	Yes	Yes
Automated End of Day processing (UC4)	Orchestration & Job Scheduling	Yes	Yes
Terminal Services Gateway (Microsoft Terminal Server)	Jump Point, Remote Access, Virtualization	Yes	Yes
Wormhole (Secure Shell)	Jump Point, Remote Access, Virtualization	Yes	Yes
Management Application (Check MK)	Management	Yes	Yes

Indirect SCI System Categories are described below.

[392] Source: *Standard – Indirect SCI Systems*. For the avoidance of doubt, should the information in this appendix related to ISE Indirect SCI Systems at any time conflict with the policy *Standard – Indirect SCI Systems*, the policy supersedes and this appendix must be updated promptly.

[393] An assailable protocol is any protocol that can be used to modify SCI systems configuration or data.

APPENDIX E: INDIRECT SCI SYSTEMS[394] (*Cont'd*)

Below are the descriptions for the various Indirect SCI System Categories:

INDIRECT SYSTEM CATEGORY	DESCRIPTION
Central Database and File Shares	Services responsible for, including and not limited to, access to SCI Systems for data transfer and storage.
Cybersecurity controls	Services responsible for, including and not limited to, defending SCI Systems, providing authentication and authorization services, and security information and event monitoring.
Jump Hosts, Citrix & Remote Access:	Services responsible for, including and not limited to, access to SCI Systems for administration, market surveillance, computer operations, application operations, network operations, security operations, and market operations.
Management	Services responsible for, including and not limited to, snmp read-write access to SCI Systems, data access (log pulls), alerting, and event management requiring read-write access. For example, snmp read-only would be a non-assailable protocol, for monitoring only, and not in scope.
Orchestration & Job Scheduling	Services responsible for, including and not limited to, executing pre-defined scripts and job schedules such as opening and closing the marketplace, end-of-day processing, and facilitating data transfer in and out of SCI Systems. Orchestration and job scheduling are typically considered separate concerns. Both concerns can affect system configuration and are combined for simplicity.

[394] Source: *Standard – Indirect SCI Systems*. For the avoidance of doubt, should the information in this appendix related to ISE Indirect SCI Systems at any time conflict with the policy *Standard – Indirect SCI Systems*, the policy supersedes and this appendix must be updated promptly.

APPENDIX F-1: THIRD PARTY – FINRA REGULATION SCI POLICIES AND PROCEDURES

The documents listed below outline the FINRA policies and procedures developed for Regulation SCI with respect to RSA systems and provided to ISE via email on September 30, 2015.

DOCUMENT TITLE	DOCUMENT OVERVIEW, SCOPE, PURPOSE OR OTHER INTRODUCTORY LANGUAGE.
Regulation SCI Policies and Procedures for Periodic Review of the Effectiveness of Written Policies and Procedures and Recordkeeping Requirements	**Overview & Scope** This document sets forth FINRA's policies and procedures regarding the following areas for SCI systems: • Periodic review of the effectiveness of written policies and procedures, establishment of criteria to be used to perform the review, and establishment of a system for documenting prompt corrective action taken to remedy deficiencies in policies and procedures. (Rule 1001(a)(3), Rule 1001(c)(2) and Rule 1002(b)(3)). • Recordkeeping Requirements (Rule 1005(a)).
Regulation SCI Policies and Procedures concerning Responsible SCI Personnel	**General Overview and Purpose** Regulation SCI requires FINRA to, among other things, "establish, maintain, and enforce reasonably designed written policies and procedures that include the criteria for identifying responsible SCI personnel, the designation and documentation of responsible SCI personnel, and escalation procedures to quickly inform responsible SCI personnel of potential SCI events (SCI Rule 1001(c)(1)).
Regulation Systems, Compliance, and Integrity – FINRA Technology Policies and Procedures	Rule 1001(a) requires each SCI entity to establish, maintain, and enforce written policies and procedures to ensure that all SCI systems and indirect SCI systems have levels of capacity, integrity, resiliency, availability, and security adequate to maintain the SCI entity's operational capability and promote the maintenance of fair and orderly markets. Periodic review by an SCI entity of the effectiveness of its policies and procedures and prompt action by the SCI entity to remedy deficiencies in such policies and procedures is demanded by Rule 1001(a). **Comment.** APPENDIX A to this document lists FINRA's policies and procedures that satisfy the 7 minimum elements of Rule 1001(a)(2).
Regulation SCI Policies and Procedures for Intrusion Reporting	**Purpose** This document is a guideline and does not establish any policy or formal procedure. It is intended to serve two purposes: 1) It provides information and guidance to InfoSec staff, and 2) some of the information in this document is intended to be incorporated into FINRA's formal SCI policy and procedure documents.
Regulation SCI Policies and Procedures – FINRA Market Regulation SCI Systems	**Overview & Scope** The term "SCI systems" in this document is limited to those FINRA SCI systems operating in a FINRA production environment that support FINRA's market regulation or market surveillance activities. These procedures do not cover SCI systems – including those operating in the FINRA production

DOCUMENT TITLE	DOCUMENT OVERVIEW, SCOPE, PURPOSE OR OTHER INTRODUCTORY LANGUAGE.
	environment – for which the Transparency Services department is responsible, as identified in the FINRA Application Gold Source. These procedures also do not cover FINRA indirect SCI systems. Polies and procedures for excluded SCI systems are covered by other documents. This document sets forth FINRA's policies and procedures covering the following sections of Reg SCI for SCI systems: • Systems Compliance (Rule 1001(b)); • SCI Event Definitions and SCI Event Monitoring, Detection and Escalation (Rule 1001(a)(2)(vii)) for SCI Disruption and Compliance Events • SCI Event Obligations – Corrective Action, Commission Notification and Dissemination (Rule 1002) for SCI Disruption and Compliance Events; and • Notifications of SCI Systems Changes (Rule 1003(a)).

APPENDIX F-2: THIRD PARTY – EXEGY REGULATION SCI POLICIES AND PROCEDURES PURSUANT TO ISE *POLICY: THIRD PARTY PROVIDERS OF SCI SYSTEMS – EXEGY*

These documents and policies were provided to ISE by Exegy (via email on October 1, 2015) pursuant to ISE's *Policy: Third Party Providers of SCI Systems – Exegy.*

EXEGY DOCUMENT NUMBER OR TYPE	DESCRIPTION
Security Brief	Security Architecture for Exegy Appliances†
Security Brief	Reg SCI Touch Points (Exegy Managed Service Operations)††
Security Brief	Reg SCI Touch Points – Diagram††
Feature Brief	Maintenance Feed Check Valve†††
Product Brief	Product Performance Testing†††
COM001	Policy and Procedure Reviews Policy††††
COM005	Business Continuity and Disaster Recovery Policy††††
COM007	Non-De Minimis SCI Events Communication and Reporting Policy††††
COM008	SCI Systems Review and Testing Policy††††
COM010	Compliance Review with SCI Entity Policy††††
LOG001	Exegy Manufacturing Test Policy and Procedure††††
MSS001	Change Management Policy††††
MSS002	Exegy Systems Monitoring Policy††††
MSS003	SCI Events Corrective Actions Policy††††
MSS004	Material Changes to Exegy SCI Systems Policy††††
MSS005	Penetration Testing Policy††††
PE001	Exegy Capacity Test Policy and Procedure††††
PE002	System Performance Testing Procedure††††
PE003	System Testing Procedure

† - Document labeled "*Exegy proprietary, subject to non-disclosure.*"

†† - Document labeled "*Confidential Information of Exegy, Inc., Subject to Non-Disclosure.*"

††† - Document labeled "*Exegy confidential and proprietary, subject to non-disclosure.*"

†††† - Document labeled "*Confidential Information of Exegy, Inc.*"

APPENDIX G: CURRENT SCI INDUSTRY STANDARDS MAPPING

Rule 1001(a)(4), *Obligations related to policies and procedures of SCI entities – Capacity, integrity, resiliency, availability, and security*, states that ISE's Rule 1001(a)(1), *Capacity, integrity, resiliency, availability, and security*, policies and procedures will be deemed reasonably designed if they are consistent with current industry standards. See *Current SCI Industry Standards: Rule 1001(a)(4)*, above.

The chart below maps ISE's Rule 1001(a)(2) minimum policies and procedures required to satisfy Rule 1001(a)(1) to current SCI industry standards.[395]

SCI RULE: SUBEJCT MATTER	ISE POLICY	SCI INDUSTRY STANDARD DOMAIN	SCI INDUSTRY STANDARD PUBLICATION MAPPED TO
Rule 1001(a)(2)(i): Technological infrastructure capacity planning estimates.	*ISE Capacity Planning*	Capacity Planning	FFIEC, Operations IT Examination Handbook (July 2004)
Rule 1001(a)(2)(ii): Periodic capacity stress tests.	*ISE Capacity Planning*	Capacity Planning	FFIEC, Operations IT Examination Handbook (July 2004)
Rule 1001(a)(2)(iii): Systems development and testing methodology	*Development and Automation Services – Software Development Methodology*	Systems Development Methodology	Institute of Electrical and Electronics Engineers (IEEE)
Rule 1001(a)(2)(iv): Regular reviews and testing.	*Procedure: Vulnerability Scanning and Patch Management*	Physical Security	NIST 800-40
	ISE Standard: Corporate Physical Security		NIST 800-53 Revision 4
Rule 1001(a)(2)(v): Business continuity and disaster recovery plans.	*Business Continuity Management Program Strategy*	Contingency Planning (BCP)	NIST Contingency Planning Guide (SP800-34) 2003 Interagency White Paper on Sound Practices SEC Policy Statement: BCP for Trading Markets
	ISE Disaster Recovery Plan		NIST Special Publication 800-34 Contingency Planning Guide from US Department of Commerce

[395] For any industry standard publication cited below that is not a listed publication in the Staff Guidance, ISE's determination to use these alternative standards in developing its policies and procedures does not necessarily mean that ISE's policies and procedures are deficient or unreasonable for purposes of Rule 1001(a)(1), *Capacity, integrity, resiliency, availability, and security*. See Adopting Release at p. 193.

SCI RULE: SUBEJCT MATTER	ISE POLICY	SCI INDUSTRY STANDARD DOMAIN	SCI INDUSTRY STANDARD PUBLICATION MAPPED TO
Rule 1001(a)(2)(vi): Design and development standards.	*Development and Automation Services – Software Development Methodology*	Systems Development Methodology	Institute of Electrical and Electronics Engineers (IEEE).
Rule 1001(a)(2)(vii): Systems monitoring.	*Policy: Information Security Incident Management*	Information Security and Networking	NIST Special Publication 800-61

APPENDIX H: ISE Members Designated for Annual Functional and Performance Testing – Rule 1004(b)

The below list of designated PMMs and EAMs Linkage Handlers shall be reviewed and updated annually prior to the planned date for ISE's annual Rule 1004(b) functional and performance testing with designated members.[396]

DESIGNATED MEMBER	CATEGORY	EXCHANGE(S)	BIN(S)
PRIMARY MARKET MAKERS (PMMs)			
Barclays Capital, Inc.	PMM	ISE Gemini	38
Citadel Securities LLC	PMM	ISE	4, 6, & 8
Citadel Securities LLC	PMM	ISE Gemini	35
Citigroup Derivatives Markets Inc.	PMM	ISE	1 & 3
Goldman, Sachs & Co.	PMM	ISE	2 & 9
Goldman, Sachs & Co.	PMM	ISE Gemini	34
Group One Trading LP	PMM	ISE Gemini	37
KCG Americas, LLC	PMM	ISE	5
KCG Americas, LLC	PMM	ISE Gemini	39
Morgan Stanley & Co, LLC	PMM	ISE	10
Morgan Stanley & Co, LLC	PMM	ISE Gemini	32
Susquehanna Securities	PMM	ISE Gemini	33
Timber Hill LLC	PMM	ISE	7
Timber Hill LLC	PMM	ISE Gemini	36
Wolverine Trading, LLC	PMM	ISE Gemini	31
ELECTRONIC ACCESS MEMBERS (EAMs) **LINKAGE HANDLERS**			
Merrill Lynch, Pierce, Fenner & Smith, Inc.	EAM Linkage Handler	▪ ISE ▪ ISE Gemini	*Not applicable*
Wolverine Execution Services, LLC	EAM Linkage Handler	▪ ISE ▪ ISE Gemini	*Not applicable*

Source: Senior Legal & Regulatory Associate, ISE Legal Department.

The above list is effective and current as of September 30, 2015.

[396] **THIS SECTION WILL HAVE TO BE REVISED.** At the request of Business Development we will be changing the criteria for designating members to participate in BC/DR testing. A proposal will be submitted to the Board next week and then filed with the SEC. [Per Claire McG, 11-6-15]

APPENDIX I: REGULATION SCI RULES 1000 – 1007

REGULATION SCI – SYSTEMS, COMPLIANCE AND INTEGRITY *Effective Date*: February 3, 2015	
Rule	**Description**
242.1000	Definitions.
242.1001	Obligations related to policies and procedures of SCI entities.
242.1002	Obligations related to SCI events.
242.1003	Obligations related to systems changes; SCI review.
242.1004	SCI entity business continuity and disaster recovery plans testing requirements for members or participants.
242.1005	Recordkeeping requirements related to compliance with Regulation SCI.
242.1006	Electronic filing and submission.
242.1007	Requirements for service bureaus.

§ 242.1000 Definitions.

For purposes of Regulation SCI (§§ 242.1000 through 242.1007), the following definitions shall apply:

Critical SCI systems means any SCI systems of, or operated by or on behalf of, an SCI entity that:

(1) Directly support functionality relating to:

(i) Clearance and settlement systems of clearing agencies;

(ii) Openings, reopenings, and closings on the primary listing market;

(iii) Trading halts;

(iv) Initial public offerings;

(v) The provision of consolidated market data; or

(vi) Exclusively-listed securities; or

(2) Provide functionality to the securities markets for which the availability of alternatives is significantly limited or nonexistent and without which there would be a material impact on fair and orderly markets.

Electronic signature has the meaning set forth in §240.19b-4(j) of this chapter.

Exempt clearing agency subject to ARP means an entity that has received from the Commission an exemption from registration as a clearing agency under Section 17A of the Act, and whose exemption contains conditions that relate to the Commission's Automation Review Policies (ARP), or any Commission regulation that supersedes or replaces such policies.

Indirect SCI systems means any systems of, or operated by or on behalf of, an SCI entity that, if breached, would be reasonably likely to pose a security threat to SCI systems.

Major SCI event means an SCI event that has had, or the SCI entity reasonably estimates would have:

(1) Any impact on a critical SCI system; or

(2) A significant impact on the SCI entity's operations or on market participants.

Plan processor has the meaning set forth in §242.600(b)(55).

Responsible SCI personnel means, for a particular SCI system or indirect SCI system impacted by an SCI event, such senior manager(s) of the SCI entity having responsibility for such system, and their designee(s).

SCI alternative trading system or SCI ATS means an alternative trading system, as defined in §242.300(a), which during at least four of the preceding six calendar months:

(1) Had with respect to NMS stocks:

(i) Five percent (5%) or more in any single NMS stock, and one-quarter percent (0.25%) or more in all NMS stocks, of the average daily dollar volume reported by applicable transaction reporting plans; or

(ii) One percent (1%) or more in all NMS stocks of the average daily dollar volume reported by applicable transaction reporting plans; or

(2) Had with respect to equity securities that are not NMS stocks and for which transactions are reported to a self-regulatory organization, five percent (5%) or more of the average daily dollar volume as calculated by the self-regulatory organization to which such

transactions are reported;

(3) Provided, however, that such SCI ATS shall not be required to comply with the requirements of Regulation SCI until six months after satisfying any of paragraphs (a) or (b) of this section, as applicable, for the first time.

SCI entity means an SCI self-regulatory organization, SCI alternative trading system, plan processor, or exempt clearing agency subject to ARP.

SCI event means an event at an SCI entity that constitutes:

(1) A systems disruption;

(2) A systems compliance issue; or

(3) A systems intrusion.

SCI review means a review, following established procedures and standards, that is performed by objective personnel having appropriate experience to conduct reviews of SCI systems and indirect SCI systems, and which review contains:

(1) A risk assessment with respect to such systems of an SCI entity; and

(2) An assessment of internal control design and effectiveness of its SCI systems and indirect SCI systems to include logical and physical security controls, development processes, and information technology governance, consistent with industry standards.

SCI self-regulatory organization or SCI SRO means any national securities exchange, registered securities association, or registered clearing agency, or the Municipal Securities Rulemaking Board; provided however, that for purposes of this section, the term SCI self-regulatory organization shall not include an exchange that is notice registered with the Commission pursuant to 15 U.S.C. 78f(g) or a limited purpose national securities association registered with the Commission pursuant to 15 U.S.C. 78o-3(k).

SCI systems means all computer, network, electronic, technical, automated, or similar systems of, or operated by or on behalf of, an SCI entity that, with respect to securities, directly support trading, clearance and settlement, order routing, market data, market regulation, or market surveillance.

Senior management means, for purposes of Rule 1003(b), an SCI entity's Chief Executive Officer, Chief Technology Officer, Chief Information Officer, General Counsel, and Chief Compliance Officer, or the equivalent of such employees or officers of an SCI entity.

Systems compliance issue means an event at an SCI entity that has caused any SCI system of such entity to operate in a manner that does not comply with the Act and the rules and regulations thereunder or the entity's rules or governing documents, as applicable.

Systems disruption means an event in an SCI entity's SCI systems that disrupts, or significantly degrades, the normal operation of an SCI system.

Systems intrusion means any unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity.

§ 242.1001 Obligations related to policies and procedures of SCI entities.

(a) Capacity, integrity, resiliency, availability, and security. (1) Each SCI entity shall establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its SCI systems and, for purposes of security standards, indirect SCI systems, have levels of capacity, integrity, resiliency, availability, and security, adequate to maintain the SCI entity's operational capability and promote the maintenance of fair and orderly markets.

(2) Policies and procedures required by paragraph (a)(1) of this section shall include, at a minimum:

(i) The establishment of reasonable current and future technological infrastructure capacity planning estimates;

(ii) Periodic capacity stress tests of such systems to determine their ability to process transactions in an accurate, timely, and efficient manner;

(iii) A program to review and keep current systems development and testing methodology for such systems;

(iv) Regular reviews and testing, as applicable, of such systems, including backup systems, to identify vulnerabilities pertaining to internal and external threats, physical hazards,

and natural or manmade disasters;

(v) Business continuity and disaster recovery plans that include maintaining backup and recovery capabilities sufficiently resilient and geographically diverse and that are reasonably designed to achieve next business day resumption of trading and two-hour resumption of critical SCI systems following a wide-scale disruption;

(vi) Standards that result in such systems being designed, developed, tested, maintained, operated, and surveilled in a manner that facilitates the successful collection, processing, and dissemination of market data; and

(vii) Monitoring of such systems to identify potential SCI events.

(3) Each SCI entity shall periodically review the effectiveness of the policies and procedures required by this paragraph (a), and take prompt action to remedy deficiencies in such policies and procedures.

(4) For purposes of this paragraph (a), such policies and procedures shall be deemed to be reasonably designed if they are consistent with current SCI industry standards, which shall be comprised of information technology practices that are widely available to information technology professionals in the financial sector and issued by an authoritative body that is a U.S. governmental entity or agency, association of U.S. governmental entities or agencies, or widely recognized organization. Compliance with such current SCI industry standards, however, shall not be the exclusive means to comply with the requirements of this paragraph (a).

(b) Systems compliance. (1) Each SCI entity shall establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its SCI systems operate in a manner that complies with the Act and the rules and regulations thereunder and the entity's rules and governing documents, as applicable.

(2) Policies and procedures required by paragraph (b)(1) of this section shall include, at a minimum:

(i) Testing of all SCI systems and any changes to SCI systems prior to implementation;

(ii) A system of internal controls over changes to SCI systems;

(iii) 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 Act and the rules and regulations thereunder and the SCI entity's rules and governing documents; and

(iv) A plan of coordination and communication between regulatory and other personnel of the SCI entity, including by responsible SCI personnel, regarding SCI systems design, changes, testing, and controls designed to detect and prevent systems compliance issues.

(3) Each SCI entity shall periodically review the effectiveness of the policies and procedures required by this paragraph (b), and take prompt action to remedy deficiencies in such policies and procedures.

(4) Safe harbor from liability for individuals. Personnel of an SCI entity shall be deemed not to have aided, abetted, counseled, commanded, caused, induced, or procured the violation by an SCI entity of this paragraph (b) if the person:

(i) Has reasonably discharged the duties and obligations incumbent upon such person by the SCI entity's policies and procedures; and

(ii) Was without reasonable cause to believe that the policies and procedures relating to an SCI system for which such person was responsible, or had supervisory responsibility, were not established, maintained, or enforced in accordance with this paragraph (b) in any material respect.

(c) Responsible SCI personnel. (1) Each SCI entity shall establish, maintain, and enforce reasonably designed written policies and procedures that include the criteria for identifying responsible SCI personnel, the designation and documentation of responsible SCI personnel, and escalation procedures to quickly inform responsible SCI personnel of potential SCI events.

(2) Each SCI entity shall periodically review the effectiveness of the policies and procedures required by paragraph (c)(1) of this section, and take prompt action to remedy deficiencies in such policies and procedures.

§ 242.1002 Obligations related to SCI events.

(a) Corrective action. Upon any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred, each SCI entity shall begin to take appropriate corrective action which shall include, at a minimum, mitigating potential harm to investors and market integrity resulting from the SCI event and devoting adequate resources to remedy the SCI event as soon as reasonably practicable.

(b) Commission notification and recordkeeping of SCI events. Each SCI entity shall:

(1) Upon any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred, notify the Commission of such SCI event immediately;

(2) Within 24 hours of any responsible SCI personnel having a reasonable basis to conclude that the SCI event has occurred, submit a written notification pertaining to such SCI event to the Commission, which shall be made on a good faith, best efforts basis and include:

(i) A description of the SCI event, including the system(s) affected; and

(ii) To the extent available as of the time of the notification: the SCI entity's current assessment of the types and number of market participants potentially affected by the SCI event; the potential impact of the SCI event on the market; a description of the steps the SCI entity has taken, is taking, or plans to take, with respect to the SCI event; the time the SCI event was resolved or timeframe within which the SCI event is expected to be resolved; and any other pertinent information known by the SCI entity about the SCI event;

(3) Until such time as the SCI event is resolved and the SCI entity's investigation of the SCI event is closed, provide updates pertaining to such SCI event to the Commission on a regular basis, or at such frequency as reasonably requested by a representative of the Commission, to correct any materially incorrect information previously provided, or when new material information is discovered, including but not limited to, any of the information listed in paragraph (b)(2)(ii) of this section;

(4)(i)(A) If an SCI event is resolved and the SCI entity's investigation of the SCI event is closed within 30 calendar days of the occurrence of the SCI event, then within five business days after the resolution of the SCI event and closure of the investigation regarding the SCI event, submit a final written notification pertaining to such SCI event to the Commission containing the information required in paragraph (b)(4)(ii) of this section.

(B)(1) If an SCI event is not resolved or the SCI entity's investigation of the SCI event is not closed within 30 calendar days of the occurrence of the SCI event, then submit an interim written notification pertaining to such SCI event to the Commission within 30 calendar days after the occurrence of the SCI event containing the information required in paragraph (b)(4)(ii) of this section, to the extent known at the time.

(2) Within five business days after the resolution of such SCI event and closure of the investigation regarding such SCI event, submit a final written notification pertaining to such SCI event to the Commission containing the information required in paragraph (b)(4)(ii) of this

section.

(ii) Written notifications required by paragraph (b)(4)(i) of this section shall include:

(A) A detailed description of: the SCI entity's assessment of the types and number of market participants affected by the SCI event; the SCI entity's assessment of the impact of the SCI event on the market; the steps the SCI entity has taken, is taking, or plans to take, with respect to the SCI event; the time the SCI event was resolved; the SCI entity's rule(s) and/or governing document(s), as applicable, that relate to the SCI event; and any other pertinent information known by the SCI entity about the SCI event;

(B) A copy of any information disseminated pursuant to paragraph (c) of this section by the SCI entity to date regarding the SCI event to any of its members or participants; and

(C) An analysis of parties that may have experienced a loss, whether monetary or otherwise, due to the SCI event, the number of such parties, and an estimate of the aggregate amount of such loss.

(5) The requirements of paragraphs (b)(1) through (4) of this section shall not apply to any SCI event that has had, or the SCI entity reasonably estimates would have, no or a de minimis impact on the SCI entity's operations or on market participants. For such events, each SCI entity shall:

(i) Make, keep, and preserve records relating to all such SCI events; and

(ii) Submit to the Commission a report, within 30 calendar days after the end of each calendar quarter, containing a summary description of such systems disruptions and systems intrusions, including the SCI systems and, for systems intrusions, indirect SCI systems, affected by such systems disruptions and systems intrusions during the applicable calendar quarter.

(c) Dissemination of SCI events. (1) Each SCI entity shall:

(i) Promptly after any responsible SCI personnel has a reasonable basis to conclude that an SCI event that is a systems disruption or systems compliance issue has occurred, disseminate the following information about such SCI event:

(A) The system(s) affected by the SCI event; and

(B) A summary description of the SCI event; and

(ii) When known, promptly further disseminate the following information about such SCI event:

(A) A detailed description of the SCI event;

(B) The SCI entity's current assessment of the types and number of market participants potentially affected by the SCI event; and

(C) A description of the progress of its corrective action for the SCI event and when the SCI event has been or is expected to be resolved; and

(iii) Until resolved, provide regular updates of any information required to be disseminated under paragraphs (c)(1)(i) and (ii) of this section.

(2) Each SCI entity shall, promptly after any responsible SCI personnel has a reasonable basis to conclude that a SCI event that is a systems intrusion has occurred, disseminate a summary description of the systems intrusion, including a description of the corrective action taken by the SCI entity and when the systems intrusion has been or is expected to be resolved, unless the SCI entity determines that dissemination of such information would likely compromise the security of the SCI entity's SCI systems or indirect SCI systems, or an investigation of the systems intrusion, and documents the reasons for such determination.

(3) The information required to be disseminated under paragraphs (c)(1) and (2) of this section promptly after any responsible SCI personnel has a reasonable basis to conclude that an SCI event has occurred, shall be promptly disseminated by the SCI entity to those members or participants of the SCI entity that any responsible SCI personnel has reasonably estimated may have been affected by the SCI event, and promptly disseminated to any additional members or participants that any responsible SCI personnel subsequently reasonably estimates may have been affected by the SCI event; provided, however, that for major SCI events, the information required to be disseminated under paragraphs (c)(1) and (2) of this section shall be promptly disseminated by the SCI entity to all of its members or participants.

(4) The requirements of paragraphs (c)(1) through (3) of this section shall not apply to:

(i) SCI events to the extent they relate to market regulation or market surveillance systems; or

(ii) Any SCI event that has had, or the SCI entity reasonably estimates would have, no or a de minimis impact on the SCI entity's operations or on market participants.

§ 242.1003 Obligations related to systems changes; SCI review.

(a) Systems changes. Each SCI entity shall:

(1) Within 30 calendar days after the end of each calendar quarter, submit to the

Commission a report describing completed, ongoing, and planned material changes to its SCI systems and the security of indirect SCI systems, during the prior, current, and subsequent calendar quarters, including the dates or expected dates of commencement and completion. An SCI entity shall establish reasonable written criteria for identifying a change to its SCI systems and the security of indirect SCI systems as material and report such changes in accordance with such criteria.

(2) Promptly submit a supplemental report notifying the Commission of a material error in or material omission from a report previously submitted under this paragraph (a).

(b) SCI review. Each SCI entity shall:

(1) Conduct an SCI review of the SCI entity's compliance with Regulation SCI not less than once each calendar year; provided, however, that:

(i) Penetration test reviews of the network, firewalls, and production systems shall be conducted at a frequency of not less than once every three years; and

(ii) Assessments of SCI systems directly supporting market regulation or market surveillance shall be conducted at a frequency based upon the risk assessment conducted as part of the SCI review, but in no case less than once every three years; and

(2) Submit a report of the SCI review required by paragraph (b)(1) of this section to senior management of the SCI entity for review no more than 30 calendar days after completion of such SCI review; and

(3) Submit to the Commission, and to the board of directors of the SCI entity or the equivalent of such board, a report of the SCI review required by paragraph (b)(1) of this section, together with any response by senior management, within 60 calendar days after its submission to senior management of the SCI entity.

§ 242.1004 SCI entity business continuity and disaster recovery plans testing requirements for members or participants.

With respect to an SCI entity's business continuity and disaster recovery plans, including its backup systems, each SCI entity shall:

(a) Establish standards for the designation of those members or participants that the SCI entity reasonably determines are, taken as a whole, the minimum necessary for the maintenance

of fair and orderly markets in the event of the activation of such plans;

(b) Designate members or participants pursuant to the standards established in paragraph (a) of this section and require participation by such designated members or participants in scheduled functional and performance testing of the operation of such plans, in the manner and frequency specified by the SCI entity, provided that such frequency shall not be less than once every 12 months; and

(c) Coordinate the testing of such plans on an industry- or sector-wide basis with other SCI entities.

§ 242.1005 Recordkeeping requirements related to compliance with Regulation SCI.

(a) An SCI SRO shall make, keep, and preserve all documents relating to its compliance with Regulation SCI as prescribed in §240.17a-1 of this chapter.

(b) An SCI entity that is not an SCI SRO shall:

(1) Make, keep, and preserve at least one copy of all documents, including correspondence, memoranda, papers, books, notices, accounts, and other such records, relating to 2its compliance with Regulation SCI, including, but not limited to, records relating to any changes to its SCI systems and indirect SCI systems;

(2) Keep all such documents for a period of not less than five years, the first two years in a place that is readily accessible to the Commission or its representatives for inspection and examination; and

(3) Upon request of any representative of the Commission, promptly furnish to the possession of such representative copies of any documents required to be kept and preserved by it pursuant to paragraphs (b)(1) and (2) of this section.

(c) Upon or immediately prior to ceasing to do business or ceasing to be registered under the Securities Exchange Act of 1934, an SCI entity shall take all necessary action to ensure that the records required to be made, kept, and preserved by this section shall be accessible to the Commission and its representatives in the manner required by this section and for the remainder

of the period required by this section.

§ 242.1006 Electronic filing and submission.

(a) Except with respect to notifications to the Commission made pursuant to § 242.1002(b)(1) or updates to the Commission made pursuant to paragraph § 242.1002(b)(3), any notification, review, description, analysis, or report to the Commission required to be submitted under Regulation SCI shall be filed electronically on Form SCI (§249.1900 of this chapter), include all information as prescribed in Form SCI and the instructions thereto, and contain an electronic signature; and

(b) The signatory to an electronically filed Form SCI shall manually sign a signature page or document, in the manner prescribed by Form SCI, authenticating, acknowledging, or otherwise adopting his or her signature that appears in typed form within the electronic filing. Such document shall be executed before or at the time Form SCI is electronically filed and shall be retained by the SCI entity in accordance with § 242.1005.

§ 242.1007 Requirements for service bureaus.

If records required to be filed or kept by an SCI entity under Regulation SCI are prepared or maintained by a service bureau or other recordkeeping service on behalf of the SCI entity, the SCI entity shall ensure that the records are available for review by the Commission and its representatives by submitting a written undertaking, in a form acceptable to the Commission, by such service bureau or other recordkeeping service, signed by a duly authorized person at such service bureau or other recordkeeping service. Such a written undertaking shall include an agreement by the service bureau to permit the Commission and its representatives to examine such records at any time or from time to time during business hours, and to promptly furnish to the Commission and its representatives true, correct, and current electronic files in a form acceptable to the Commission or its representatives or hard copies of any or all or any part of such records, upon request, periodically, or continuously and, in any case, within the same time periods as would apply to the SCI entity for such records. The preparation or maintenance of records by a service bureau or other recordkeeping service shall not relieve an SCI entity from

its obligation to prepare, maintain, and provide the Commission and its representatives access to such records.

APPENDIX J-1: Form SCI

Subpart T—Form SCI, for filing notices and reports as required by Regulation SCI.

§ 249.1900. Form SCI, for filing notices and reports as required by Regulation SCI.

Form SCI shall be used to file notices and reports as required by Regulation SCI (§§ 242.1000 through 242.1007).

[**Note**: The text of Form SCI does not, and the amendments will not, appear in the Code of Federal Regulations.]

OMB Number:
Expiration Date:
Estimated Average burden hours per response.....

Securities and Exchange Commission
Washington, DC 20549
Form SCI

Page 1 of _____ File No. SCI-{name}-YYYY-###

SCI Notification and Reporting by: {SCI entity name}

Pursuant to Rules 1002 and 1003 of Regulation SCI under the Securities Exchange Act of 1934

- ❑ Initial
- ❑ Withdrawal

SECTION I: Rule 1002 - Commission Notification of SCI Event

A. Submission Type (select one only)

- ❑ Rule 1002(b)(1) Initial Notification of SCI event
- ❑ Rule 1002(b)(2) Notification of SCI event
- ❑ Rule 1002(b)(3) Update of SCI event: ####
- ❑ Rule 1002(b)(4) Final Report of SCI Event
- ❑ Rule 1002(b)(4) Interim Status Report of SCI event

If filing a Rule 1002(b)(1) or Rule 1002(b)(3) submission, please provide a brief description:

_____
_____
_____

B. SCI Event Type(s) (select all that apply)

- ❑ Systems compliance issue
- ❑ Systems disruption
- ❑ Systems intrusion

C. General Information Required for (b)(2) filings.

1) Has the Commission previously been notified of the SCI event pursuant to 1002(b)(1)? *yes/no*

2) Date/time SCI event occurred: *mm/dd/yyyy hh:mm am/pm*

3) Duration of SCI event: *hh:mm*, or *days*

4) Please provide the date and time when a responsible SCI personnel had reasonable basis to conclude the SCI event occurred:

mm/dd/yyyy *hh:mm am/pm*

5) Has the SCI event been resolved? *yes/no*

a) If yes, provide date and time of resolution: *mm/dd/yyyy* *hh:mm am/pm*

6) Is the investigation of the SCI event closed? *yes/no*

a) If yes, provide date of closure: *mm/dd/yyyy*

7) Estimated number of market participants potentially affected by the SCI event: ####

8) Is the SCI event a major SCI event (as defined in Rule 1000)? *yes/no*

D. Information about impacted systems:

Name(s) of system(s):

_____

_____

_____

Type(s) of system(s) impacted by the SCI event (check all that apply):

❑ Trading ❑ Clearance and settlement ❑ Order routing

❑ Market data ❑ Market regulation ❑ Market surveillance

❑ Indirect SCI systems (please describe):

_____

_____

_____

Are any critical SCI systems impacted by the SCI event (check all that apply)? Yes/No

1) Systems that directly support functionality relating to:

❑ Clearance and settlement systems of clearing agencies

❑ Openings, reopenings, and closings on the primary listing market

❑ Trading halts ❑ Initial public offerings

❑ The provision of consolidated market data ❑ Exclusively-listed securities

2) ❑ Systems that provide functionality to the securities markets for which the availability of alternatives is significantly limited or nonexistent and without which there would be a material impact on fair and orderly markets (please describe):

_____

_____

_____

SECTION II: Periodic Reporting (select one only)

A. Quarterly Reports: For the quarter ended: mm/dd/yyyy

❑ Rule 1002(b)(5)(ii): Quarterly report of systems disruptions and systems intrusions with no or a de minimis impact.

❑ Rule 1003(a)(1): Quarterly report of material systems changes

❑ Rule 1003(a)(2): Supplemental report of material systems changes

B. SCI Review Reports

❑ Rule 1003(b)(3): Report of SCI review, together with any response by senior management

Date of completion of SCI review: *mm/dd/yyyy*

Date of submission of SCI review to senior management: *mm/dd/yyyy*

SECTION III: Contact Information

Provide the following information of the person at the {SCI entity name} prepared to respond to questions for this submission:

First Name: Last Name:

Title:

E-Mail:

Telephone: Fax:

Additional Contacts (Optional)

First Name: Last Name:

Title:

E-Mail:

Telephone: Fax:

First Name: Last Name:

Title:

E-Mail:

Telephone: Fax:

SECTION IV: Signature

Confidential treatment is requested pursuant to Rule 24b-2(g). Additionally, pursuant to the requirements of the Securities Exchange Act of 1934, {SCI Entity name} has duly caused this {notification}{report} to be signed on its behalf by the undersigned duly authorized officer:

Date:

By (Name) Title (_____)

"Digitally Sign and Lock Form"

APPENDIX J-2: Form SCI – Schedule of Exhibits

Exhibit 1: **Rule 1002(b)(2)** **Notification of SCI Event** Add/Remove/View	Within 24 hours of any responsible SCI personnel having a reasonable basis to conclude that the SCI event has occurred, the SCI entity shall submit a written notification pertaining to such SCI event to the Commission, which shall be made on a good faith, best efforts basis and include: (a) a description of the SCI event, including the system(s) affected; and (b) to the extent available as of the time of the notification: the SCI entity's current assessment of the types and number of market participants potentially affected by the SCI event; the potential impact of the SCI event on the market; a description of the steps the SCI entity has taken, is taking, or plans to take, with respect to the SCI event; the time the SCI event was resolved or timeframe within which the SCI event is expected to be resolved; and any other pertinent information known by the SCI entity about the SCI event.
Exhibit 2: **Rule 1002(b)(4)** **Final or Interim Report of SCI Event** Add/Remove/View	When submitting a final report pursuant to either Rule 1002(b)(4)(i)(A) or Rule 1002(b)(4)(i)(B)(2), the SCI entity shall include: (a) a detailed description of: the SCI entity's assessment of the types and number of market participants affected by the SCI event; the SCI entity's assessment of the impact of the SCI event on the market; the steps the SCI entity has taken, is taking, or plans to take, with respect to the SCI event; the time the SCI event was resolved; the SCI entity's rule(s) and/or governing document(s), as applicable, that relate to the SCI event; and any other pertinent information known by the SCI entity about the SCI event; (b) a copy of any information disseminated pursuant to Rule 1002(c) by the SCI entity to date regarding the SCI event to any of its members or participants; and (c) an analysis of parties that may have experienced a loss, whether monetary or otherwise, due to the SCI event, the number of such parties, and an estimate of the aggregate amount of such loss. When submitting an interim report pursuant to Rule 1002(b)(4)(i)(B)(1), the SCI entity shall include such information to the extent known at the time.
Exhibit 3: **Rule 1002(b)(5)(ii)** **Quarterly Report of De Minimis SCI Events** Add/Remove/View	The SCI entity shall submit a report, within 30 calendar days after the end of each calendar quarter, containing a summary description of systems disruptions and systems intrusions that have had, or the SCI entity reasonably estimates would have, no or a de minimis impact on the SCI entity's operations or on market participants, including the SCI systems and, for systems intrusions, indirect SCI systems, affected by such SCI events during the applicable calendar quarter.
Exhibit 4: **Rule 1003 (a)** **Quarterly Report of Systems Changes** Add/Remove/View	When submitting a report pursuant to Rule 1003(a)(1), the SCI entity shall provide a report, within 30 calendar days after the end of each calendar quarter, describing completed, ongoing, and planned material changes to its SCI systems and the security of indirect SCI systems, during the prior, current, and subsequent calendar quarters, including the dates or expected dates of commencement and completion. An SCI entity shall establish reasonable written criteria for identifying a change to its SCI systems and the security of indirect SCI systems as material and report such changes in accordance with such criteria. When submitting a report pursuant to Rule 1003(a)(2), the SCI entity shall provide a supplemental report of a material error in or material omission from a report previously submitted under Rule 1003(a)(1).
Exhibit 5: **Rule 1003(b)(3)** **Report of SCI review** Add/Remove/View	The SCI entity shall provide a report of the SCI review, together with any response by senior management, within 60 calendar days after its submission to senior management of the SCI entity.
Exhibit 6: **Optional Attachments** Add/Remove/View	This exhibit may be used in order to attach other documents that the SCI entity may wish to submit as part of a Rule 1002(b)(1) initial notification submission or Rule 1002(b)(3) update submission.

APPENDIX J-3: Form SCI – General Instructions

A. Use of the Form

Except with respect to notifications to the Commission made pursuant to Rule 1002(b)(1) or updates to the Commission made pursuant to Rule 1002(b)(3), any notification, review, description, analysis, or report required to be submitted pursuant to Regulation SCI under the Securities Exchange Act of 1934 ("Act") shall be filed in an electronic format through an electronic form filing system ("**EFFS**"), a secure website operated by the Securities and Exchange Commission ("**Commission**"). Documents attached as exhibits filed through the EFFS system must be in a text-searchable format without the use of optical character recognition. If, however, a portion of a Form SCI submission (e.g., an image or diagram) cannot be made available in a text-searchable format, such portion may be submitted in a non-text searchable format.

B. Need for Careful Preparation of the Completed Form, Including Exhibits

This form, including the exhibits, is intended to elicit information necessary for Commission Staff to work with SCI self-regulatory organizations, SCI alternative trading systems, plan processors, and exempt clearing agencies subject to ARP (collectively, "**SCI entities**") to ensure the capacity, integrity, resiliency, availability, security, and compliance of their automated systems. An SCI entity must provide all the information required by the form, including the exhibits, and must present the information in a clear and comprehensible manner. A filing that is incomplete or similarly deficient may be returned to the SCI entity. Any filing so returned shall for all purposes be deemed not to have been filed with the Commission. See also Rule 0-3 under the Act (17 CFR 240.0-3).

C. When to Use the Form

Form SCI is comprised of six types of required submissions to the Commission pursuant to Rules 1002 and 1003. In addition, Form SCI permits SCI entities to submit to the Commission two additional types of submissions pursuant to Rules 1002(b)(1) and 1002(b)(3); however, SCI entities are not required to use Form SCI for these two types of submissions to the Commission. In filling out Form SCI, an SCI entity shall select the type of filing and provide all

information required by Regulation SCI specific to that type of filing.

The first two types of required submissions relate to Commission notification of certain SCI events:

(1) "Rule 1002(b)(2) Notification of SCI Event" submissions for notifications regarding systems disruptions, systems compliance issues, or systems intrusions (collectively, "**SCI events**"), other than any systems disruption or systems intrusion that has had, or the SCI entity reasonably estimates would have, no or a de minimis impact on the SCI entity's operations or on market participants; and

(2) "Rule 1002(b)(4) Final or Interim Report of SCI Event" submissions, of which there are two kinds (a final report under Rule 1002(b)(4)(i)(A) or Rule 1002(b)(4)(i)(B)(2); or an interim status report under Rule 1002(b)(4)(i)(B)(1)).

The other four types of required submissions are periodic reports, and include:

(1) "Rule 1002(b)(5)(ii)" submissions for quarterly reports of systems disruptions and systems intrusions which have had, or the SCI entity reasonably estimates would have, no or a de minimis impact on the SCI entity's operations or on market participants ("**de minimis SCI events**");

(2) "Rule 1003(a)(1)" submissions for quarterly reports of material systems changes;

(3) "Rule 1003(a)(2)" submissions for supplemental reports of material systems changes; and

(4) "Rule 1003(b)(3)" submissions for reports of SCI reviews.

Required Submissions for SCI Events

For 1002(b)(2) submissions, an SCI entity must notify the Commission using Form SCI by selecting the appropriate box in Section I and filling out all information required by the form, including Exhibit 1. 1002(b)(2) submissions must be submitted within 24 hours of any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred.

For 1002(b)(4) submissions, if an SCI event is resolved and the SCI entity's investigation of the SCI event is closed within 30 calendar days of the occurrence of the SCI event, an SCI entity must file a final report under Rule 1002(b)(4)(i)(A) within five business days after the resolution of the SCI event and closure of the investigation regarding the SCI event. However, if an SCI event is not resolved or the SCI entity's investigation of the SCI event is not closed within 30 calendar days of the occurrence of the SCI event, an SCI entity must file an interim

status report under Rule 1002(b)(4)(i)(B)(1) within 30 calendar days after the occurrence of the SCI event. For SCI events in which an interim status report is required to be filed, an SCI entity must file a final report under Rule 1002(b)(4)(i)(B)(2) within five business days after the resolution of the SCI event and closure of the investigation regarding the SCI event. For 1002(b)(4) submissions, an SCI entity must notify the Commission using Form SCI by selecting the appropriate box in Section I and filling out all information required by the form, including Exhibit 2.

Required Submissions for Periodic Reporting

For 1002(b)(5)(ii) submissions, an SCI entity must submit quarterly reports of systems disruptions and systems intrusions which have had, or the SCI entity reasonably estimates would have, no or a de minimis impact on the SCI entity's operations or on market participants. The SCI entity must select the appropriate box in Section II and fill out all information required by the form, including Exhibit 3.

For 1003(a)(1) submissions, an SCI entity must submit its quarterly report of material systems changes to the Commission using Form SCI. The SCI entity must select the appropriate box in Section II and fill out all information required by the form, including Exhibit 4.

Filings made pursuant to Rule 1002(b)(5)(ii) and Rule 1003(a)(1) must be submitted to the Commission within 30 calendar days after the end of each calendar quarter (i.e., March 31st, June 30th, September 30th and December 31st) of each year.

For 1003(a)(2) submissions, an SCI entity must submit a supplemental report notifying the Commission of a material error in or material omission from a report previously submitted under Rule 1003(a). The SCI entity must select the appropriate box in Section II and fill out all information required by the form, including Exhibit 4.

For 1003(b)(3) submissions, an SCI entity must submit its report of its SCI review, together with any response by senior management, to the Commission using Form SCI. A 1003(b)(3) submission is required within 60 calendar days after the report of the SCI review has been submitted to senior management of the SCI entity. The SCI entity must select the appropriate box in Section II and fill out all information required by the form, including Exhibit 5.

Optional Submissions

An SCI entity may, but is not required to, use Form SCI to submit a notification pursuant

to Rule 1002(b)(1). If the SCI entity uses Form SCI to submit a notification pursuant to Rule 1002(b)(1), it must select the appropriate box in Section I and provide a short description of the SCI event. Documents may also be attached as Exhibit 6 if the SCI entity chooses to do so. An SCI entity may, but is not required to, use Form SCI to submit an update pursuant to Rule 1002(b)(3). Rule 1002(b)(3) requires an SCI entity to, until such time as the SCI event is resolved and the SCI entity's investigation of the SCI event is closed, provide updates pertaining to such SCI event to the Commission on a regular basis, or at such frequency as reasonably requested by a representative of the Commission, to correct any materially incorrect information previously provided, or when new material information is discovered, including but not limited to, any of the information listed in Rule 1002(b)(2)(ii). If the SCI entity uses Form SCI to submit an update pursuant to Rule 1002(b)(3), it must select the appropriate box in Section I and provide a short description of the SCI event. Documents may also be attached as Exhibit 6 if the SCI entity chooses to do so.

D. Documents Comprising the Completed Form

The completed form filed with the Commission shall consist of Form SCI, responses to all applicable items, and any exhibits required in connection with the filing. Each filing shall be marked on Form SCI with the initials of the SCI entity, the four-digit year, and the number of the filing for the year (e.g., SCI Name-YYYY-XXX).

E. Contact Information; Signature; and Filing of the Completed Form

Each time an SCI entity submits a filing to the Commission on Form SCI, the SCI entity must provide the contact information required by Section III of Form SCI. Space for additional contact information, if appropriate, is also provided.

All notifications and reports required to be submitted through Form SCI shall be filed through the EFFS. In order to file Form SCI through the EFFS, SCI entities must request access to the Commission's External Application Server by completing a request for an external account user ID and password. Initial requests will be received by contacting (202) 551-5777. An e-mail will be sent to the requestor that will provide a link to a secure website where basic profile information will be requested. A duly authorized individual of the SCI entity shall electronically sign the completed Form SCI as indicated in Section IV of the form. In addition, a duly authorized individual of the SCI entity shall manually sign one copy of the completed Form

SCI, and the manually signed signature page shall be preserved pursuant to the requirements of Rule 1005.

F. Withdrawals of Commission Notifications and Periodic Reports

If an SCI entity determines to withdraw a Form SCI, it must complete Page 1 of the Form SCI and indicate by selecting the appropriate check box to withdraw the submission.

G. Paperwork Reduction Act Disclosure

This collection of information will be reviewed by the Office of Management and Budget in accordance with the clearance requirements of 44 U.S.C. 3507. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid control number. The Commission estimates that the average burden to respond to Form SCI will be between one and 125 hours, depending upon the purpose for which the form is being filed. Any member of the public may direct to the Commission any comments concerning the accuracy of this burden estimate and any suggestions for reducing this burden.

Except with respect to notifications to the Commission made pursuant to Rule 1002(b)(1) or updates to the Commission made pursuant to Rule 1002(b)(3), it is mandatory that an SCI entity file all notifications, reviews, descriptions, analyses, and reports required by Regulation SCI using Form SCI. The Commission will keep the information collected pursuant to Form SCI confidential to the extent permitted by law. Subject to the provisions of the Freedom of Information Act, 5 U.S.C. 522 ("**FOIA**"), and the Commission's rules thereunder (17 CFR 200.80(b)(4)(iii)), the Commission does not generally publish or make available information contained in any reports, summaries, analyses, letters, or memoranda arising out of, in anticipation of, or in connection with an examination or inspection of the books and records of any person or any other investigation.

H. Exhibits

List of exhibits to be filed, as applicable:

Exhibit 1: Rule 1002(b)(2) – Notification of SCI Event. Within 24 hours of any responsible SCI personnel having a reasonable basis to conclude that the SCI event has occurred, the SCI entity shall submit a written notification pertaining to such SCI event to the Commission, which shall be made on a good faith, best efforts basis and include: (a) a description of the SCI event,

including the system(s) affected; and (b) to the extent available as of the time of the notification: the SCI entity's current assessment of the types and number of market participants potentially affected by the SCI event; the potential impact of the SCI event on the market; a description of the steps the SCI entity has taken, is taking, or plans to take, with respect to the SCI event; the time the SCI event was resolved or timeframe within which the SCI event is expected to be resolved; and any other pertinent information known by the SCI entity about the SCI event.

Exhibit 2: Rule 1002(b)(4) – Final or Interim Report of SCI Event. When submitting a final report pursuant to either Rule 1002(b)(4)(i)(A) or Rule 1002(b)(4)(i)(B)(2), the SCI entity shall include: (a) a detailed description of: the SCI entity's assessment of the types and number of market participants affected by the SCI event; the SCI entity's assessment of the impact of the SCI event on the market; the steps the SCI entity has taken, is taking, or plans to take, with respect to the SCI event; the time the SCI event was resolved; the SCI entity's rule(s) and/or governing document(s), as applicable, that relate to the SCI event; and any other pertinent information known by the SCI entity about the SCI event; (b) a copy of any information disseminated pursuant to Rule 1002(c) by the SCI entity to date regarding the SCI event to any of its members or participants; and (c) an analysis of parties that may have experienced a loss, whether monetary or otherwise, due to the SCI event, the number of such parties, and an estimate of the aggregate amount of such loss. When submitting an interim report pursuant to Rule 1002(b)(4)(i)(B)(1), the SCI entity shall include such information to the extent known at the time.

Exhibit 3: Rule 1002(b)(5)(ii) – Quarterly Report of De Minimis SCI Events. The SCI entity shall submit a report, within 30 calendar days after the end of each calendar quarter, containing a summary description of systems disruptions and systems intrusions that have had, or the SCI entity reasonably estimates would have, no or a de minimis impact on the SCI entity's operations or on market participants, including the SCI systems and, for systems intrusions, indirect SCI systems, affected by such SCI events during the applicable calendar quarter.

Exhibit 4: Rule 1003(a) – Quarterly Report of Systems Changes. When submitting a report pursuant to Rule 1003(a)(1), the SCI entity shall provide a report, within 30 calendar days after the end of each calendar quarter, describing completed, ongoing, and planned material changes to its SCI systems and the security of indirect SCI systems, during the prior, current, and

subsequent calendar quarters, including the dates or expected dates of commencement and completion. An SCI entity shall establish reasonable written criteria for identifying a change to its SCI systems and the security of indirect SCI systems as material and report such changes in accordance with such criteria. When submitting a report pursuant to Rule 1003(a)(2), the SCI entity shall provide a supplemental report of a material error in or material omission from a report previously submitted under Rule 1003(a); provided, however, that a supplemental report is not required if information regarding a material systems change is or will be provided as part of a notification made pursuant to Rule 1002(b).

Exhibit 5: Rule 1003(b)(3) – Report of SCI Review. The SCI entity shall provide a report of the SCI review, together with any response by senior management, within 60 calendar days after its submission to senior management of the SCI entity.

Exhibit 6: Optional Attachments. This exhibit may be used in order to attach other documents that the SCI entity may wish to submit as part of a Rule 1002(b)(1) initial notification submission or Rule 1002(b)(3) update submission.

I. Explanation of Terms

Critical SCI systems means any SCI systems of, or operated by or on behalf of, an SCI entity that: (1) directly support functionality relating to: (i) clearance and settlement systems of clearing agencies; (ii) openings, reopenings, and closings on the primary listing market; (iii) trading halts; (iv) initial public offerings; (v) the provision of consolidated market data; or (vi) exclusively-listed securities; or (2) provide functionality to the securities markets for which the availability of alternatives is significantly limited or nonexistent and without which there would be a material impact on fair and orderly markets.

Indirect SCI systems means any systems of, or operated by or on behalf of, an SCI entity that, if breached, would be reasonably likely to pose a security threat to SCI systems.

Major SCI event means an SCI event that has had, or the SCI entity reasonably estimates would have: (1) any impact on a critical SCI system; or (2) a significant impact on the SCI entity's operations or on market participants.

Responsible SCI personnel means, for a particular SCI system or indirect SCI system impacted

by an SCI event, such senior manager(s) of the SCI entity having responsibility for such system, and their designee(s).

SCI entity means an SCI self-regulatory organization, SCI alternative trading system, plan processor, or exempt clearing agency subject to ARP.

SCI event means an event at an SCI entity that constitutes: (1) a systems disruption; (2) a systems compliance issue; or (3) a systems intrusion.

SCI review means a review, following established procedures and standards, that is performed by objective personnel having appropriate experience to conduct reviews of SCI systems and indirect SCI systems, and which review contains: (1) a risk assessment with respect to such systems of an SCI entity; and (2) an assessment of internal control design and effectiveness of its SCI systems and indirect SCI systems to include logical and physical security controls, development processes, and information technology governance, consistent with industry standards**.**

SCI systems means all computer, network, electronic, technical, automated, or similar systems of, or operated by or on behalf of, an SCI entity that, with respect to securities, directly support trading, clearance and settlement, order routing, market data, market regulation, or market surveillance.

Systems Compliance Issue means an event at an SCI entity that has caused any SCI system of such entity to operate in a manner that does not comply with the Act and the rules and regulations thereunder or the entity's rules or governing documents, as applicable.

Systems Disruption means an event in an SCI entity's SCI systems that disrupts, or significantly degrades, the normal operation of an SCI system.

Systems Intrusion means any unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity.

By the Commission.

Brent J. Fields,
Secretary.

Dated: November 19, 2014.