



International Securities Exchange

July 8, 2013

Elizabeth M. Murphy
Secretary
Securities and Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549

Re: Release No. 34-69077; File No. S7-01-13

Dear Ms. Murphy:

The International Securities Exchange, LLC ("ISE") is pleased to offer its comments on proposed Regulation SCI (the "Regulation").¹ The Regulation would supersede and replace the Commission's voluntary Automation Review Policy ("ARP"). The Regulation also would codify Commission and Commission staff policy positions regarding business continuity and disaster recovery ("BC/DR") plans and the reporting of system compliance issues.

The ISE supports the codification of ARP and related policies into a Commission rule. We believe that combining these policies into a single, comprehensive, rule will provide affected entities with certainty regarding their obligations in these areas under the Securities Exchange Act of 1934, as amended (the "Act"). We further believe that exposing the draft Regulation to the scrutiny of the rule-making process, including a careful cost/benefit analysis, will help ensure that the final version of the Regulation addresses the Commission's legitimate concerns in the most cost-effective manner. To help fashion the most appropriate and cost-effective Regulation, in the remainder of this letter we discuss our views on certain areas of the proposal:

- The requirement that SCI entities have plans for next-day resumption of business;
- The requirement to inform both the Commission and users of certain SCI events;
- The following operational aspects of the Regulation: periodic testing of SCI systems; the definition of "SCI security systems"; the scope of the required system change notifications; BC/DR recovery testing; the "industry standards" the Commission proposes to be used as a basis of a "safe harbor" under the Regulation; and Commission access to the production system; and
- The economic effects of the Regulation, including the cost-benefit analysis, on SCI entities and their users.

¹ Release No. 34-69077, March 8, 2013 (78 F.R. 18084, March 25, 2013) (the "Release"). Throughout this letter we use the defined terms in the Regulation.

I. Next-Day Resumption of Business

The Regulation would require exchanges to “establish, maintain and enforce written policies and procedures reasonably designed,” among other things, to provide for backup and recovery capabilities sufficiently resilient and geographically diverse to ensure next business day resumption of trading following a “wide-scale disruption.” The Commission explains that this requirement is designed to help ensure that exchanges would be able to continue operations from the backup site during disruptions such as natural disasters or terrorist activities. The Commission further explains that the Regulation does not specify any particular minimum distance or geographic location that would be necessary to achieve the requisite level of geographic diversity. Furthermore, there is the expectation that an exchange would have a reasonable degree of flexibility to determine the precise nature and location of its backup site.²

While we support the general goal of next-day business resumption, we believe that the Commission should craft this requirement in the context of the prevailing market structure in which multiple markets trade the same products. The Commission also should take into consideration the practical realities of a next-day requirement in times of stress. If the Commission does ultimately adopt a next-day trading standard, we believe the Commission should apply it in a flexible manner, relying in large part on the experiences SCI entities have had in real-life, wide-scale disruptions.

A. Competition Between Markets Provides Almost Complete Redundancy

Eighteen self-regulatory organizations (“SROs”) currently provide a market for the trading of securities: 17 exchanges and the Financial Industry Regulatory Authority (“FINRA”). Of these, 13 exchanges and FINRA provide markets for equity securities (as do, pursuant to Commission estimates, approximately 10 automated trading systems that would fall within the definition of an SCI entity³) and 11 exchanges trade listed options. No one SCI entity is dominant in its respective market segment for products traded in multiple venues. Thus, the extremely competitive nature of these markets already provides significant back-up capability in the event one or more competing markets cannot open for trading on a given day.

Despite having many markets trading the same securities, we agree with the general requirement that SCI entities should have dual processing sites. Indeed, we believe that it is best business practice for a market to have back-up disaster recovery facilities and robust BC/DR plans. We also believe that it is appropriate for the Commission to apply the goal of resuming trading on a next-day basis to SCI entities. The key is that with multiple layers of redundancy in the market the Commission should apply the next-day resumption standard in a flexible manner. In this regard, we note that the Release recognizes the Commission’s belief that “an SCI entity should have a reasonable degree of flexibility to determine the precise nature and location of its backup site depending on the particular vulnerabilities associated with those sites, and the nature, size, technology, business model, and other aspects of its business.”⁴ Thus, SCI entities like the ISE that have adopted the business model of trading securities fully available for multiple trading should have significant flexibility in applying the next-day requirement. As discussed below, this means recognizing practical realities and the real-life experiences of SCI entities in recent wide-spread disruptions.

² See *Id.* at pages 18107-18108.

³ *Id.* at page 18094.

⁴ *Id.* at note 182. Emphasis added.

B. The Regulation Must Reflect Practical Realities

In applying a next-day standard, the Commission must consider practical realities including, most importantly, the health and safety of the employees of SCI entities and their participants. The U.S. financial markets are concentrated in two metropolitan areas, New York City and Chicago. These centers house most major SCI entities, as well as the members who trade through these entities. Even markets headquartered elsewhere generally house their data centers near one or both of these locations to allow their members to connect with the lowest possible latency. A wide-scale disruption in either of these two localities, particularly New York City, will make next-day resumption of trading on a specific exchange difficult, even with all the requirements of the proposed Regulation in place.

Even if operationally ready, the markets cannot open for trading unless their members and other users also are able to trade. Since most of these entities would not be subject to the Regulation, the SCI entities could have all the operational controls and readiness in place, and be open for business on the next day, but find that significant segments of its membership would be unable or unwilling to commence trading. While the Release raises for discussion possibly expanding the scope of the Regulation to cover the broker-dealer community, that would add significant cost to the proposal and would not seem to be a reasonable first step. Thus, the Commission must analyze the practicalities of requiring one or more SCI entities to reopen the day after a wide-spread disruption given that users of such SCI entities may not be able to resume trading.

We do not approach this issue in a vacuum. The financial community has had two relatively recent experiences with wide-spread disruptions: the terrorist attacks of September 11, 2001 ("9/11") and Superstorm Sandy in October 2012 ("Sandy"). In both cases the securities markets closed for a number of days, and both offer important insights into the dependencies that arise when trying to open markets following a disruption. Approaching this from the perspective of a listed options market, ISE can open for trading only if the respective markets for the underlying products are open and our members are available to trade on the ISE.

In the aftermath of the 9/11 attacks, ISE implemented its business continuity plan. We never lost power at our New York City headquarters or at our data centers. We had the ability to operate remotely and were ready to trade throughout the event. However, practical realities delayed the opening of the markets. First, the underlying equities markets were not able to open, with certain markets sustaining physical damage to their facilities. Moreover, many of our members were unable to operate following the attacks, with many members having lost their network connections to the exchanges and some members even having lost their entire trading facilities.

Reopening the markets on an accelerated basis would have put the lives of the people who operate our markets at risk. Looking back at this event a dozen years after-the-fact obscures the issues we all faced during those days. Overall, we strongly believe that the exchanges, our members, and the Commission all acted responsibly in this time of great stress. There was no significant criticism at that time, nor should there have been, of the decision to close the markets for nearly a week.

While Sandy presents both similarities to, and differences from, 9/11, the bottom line is the same: the industry acted diligently and responsibly. While we clearly learned lessons from Sandy that can help us improve BC/DR efforts, particularly regarding the proper testing of systems and BC/DR preparedness, overall the process worked well. The main difference between 9/11 and Sandy is that the industry had advance warning

of the event and we were able to put our respective business continuity plans in effect prior to the storm. ISE did just that, stationing people at or near our BC/DR facility, preparing to be operational when the storm hit. We participated in the industry conference calls before and during the storm and we were fully capable of operating throughout the event with staff at all necessary locations.

ISE was prepared to operate throughout the Sandy event due to the manner in which we crafted our BC/DR plans. While our data centers are geographically diverse for the purposes of utilities, and, to some extent, transportation system, they are within driving distance of each other. This is critical when you ask your employees in times of stress to leave their families and loved ones at home to fulfill their employment obligations. All of our employees deployed to our BC/DR site remained within a reasonable distance of their homes, permitting a rotation of employees at the BC/DR facility during the event.

Despite these general successes during Sandy, we do appreciate that there were issues regarding at least some equity markets' preparedness to open on a fully automated basis on the anticipated day of Sandy's landfall. It is our understanding that there may not have been adequate testing of certain business continuity plans. We agree that the Regulation should address these types of concerns so that all markets have in place policies and procedures that at least provide the opportunity to remain open during a storm. While this uncertainty was a contributing factor to the markets remaining closed for two days during Sandy, it was far from the sole reason for the shut-down. Of greater importance was ensuring the health and safety of workers in the financial community during the storm.

During Sandy the government ordered significant evacuations in many parts of the New York City metropolitan area, including the lower Manhattan financial district. As noted, anticipating such restrictions, we implemented our BC/DR plan and had critical staff located at our disaster recovery site and had additional staff prepared to work from other remote locations, including their homes. However, industry discussions coordinated by the Securities Industry and Financial Markets Association ("SIFMA") made clear that member firms were not in a position to trade on the day forecasted for Sandy to reach the area. Evacuations, the closing of mass transit and many thoroughfares, and limited remote trading capabilities all contributed to this decision. The inability of our members to trade mooted any further discussion of our trading. Nothing in the proposed Regulation would negate this factor and we would not have been able to commence trading regardless of the readiness of the equity markets or the distance between our two data centers. Yet during Sandy, as during 9/11, our BC/DR plans worked and our market – on a stand-alone basis – was ready to trade.

C. There Must be a Flexible Application of the Next-Day Requirement

The lesson of 9/11 and Sandy is that the best-laid BC/DR plans and requirements always take a back seat to practical realities. The Commission must carefully evaluate the Regulation to ensure that it does not impose costs and obligations on the industry that fail to achieve the desired results in "crunch time," when SCI entities actually must implement their plans. As currently proposed, the Regulation imposes significant obligations on SCI entities to establish disaster recovery facilities and to have them available for next-day resumption of trading, and critical members will need to have connectivity to such facilities. All of this will impose significant costs on the securities market. Yet, in the event of a wide-spread disruption, health and safety of our industry's employees will remain paramount. SCI entities will not man facilities if there is an

unreasonable risk of harm. Our members may or may not have BC/DR facilities, and may or may not be connected to us. Thus, as in Sandy, we may find ourselves ready to trade, but without a critical mass of members ready, willing or able to use our markets.

In recognition of this reality, the Commission should include in the Regulation, and make clear in the adopting commentary, that it will evaluate an SCI entity's readiness to resume trading on a next-day basis flexibly, giving significant consideration to health and safety concerns. Indeed, the more remote an SCI entity's disaster recovery facility, the more difficult it would be to man such a facility in the event of a wide-spread disruption. In an event with no advanced warning, like 9/11, the more geographically diverse a site is, the less practical it would be to operate from that site if transportation and power is limited. The only way to address such a concern would be to require SCI entities to maintain staff on a full-time basis at remote sites, a hugely expensive proposition that the Regulation does not currently contemplate. Thus, recognizing that almost all securities are multiply-traded across exchanges, the best dual-site strategy for an SCI entity may well be to have the two sites in close geographic proximity, although on separate infrastructure components.

The experiences of both 9/11 and Sandy demonstrate that this flexibility is warranted. Indeed, both events show that such a strategy works.⁵ ISE has historically maintained BC/DR centers close to its New York City headquarters. In both the 9/11 and Sandy events we never lost the ability to trade, and we would have remained open if the underlying equity markets and our members were prepared to trade. We believe that this real-life experience is more important than any of the theoretical constructs on which the Commission can base its requirement for next-day operational readiness. We thus ask that the Commission make clear that significant geographic diversity is not an absolute requirement of the rule and that arrangements such as those employed by the ISE are acceptable.

II. Notice of SCI Events

The Regulation defines an "SCI event" as: a system disruption, which includes an interruption in normal service; a compliance issue, which is when an SCI entity discovers that its system does not operate in accordance with federal securities laws or the entity's own governing documents; and a system intrusion, which is an unauthorized entry into an SCI system or SCI security system. An SCI entity would need to provide notice of these SCI events both to the Commission and to the SCI entity's members. While we agree that it is generally appropriate to provide these notifications, we believe that the requirement is overly broad with respect to notice of compliance matters.

We first note that the Commission crafted the Regulation narrowly regarding two of the three reporting requirements. For system disruptions, SCI entities would need to provide members with notice only for disruptions that result in "significant harm or loss to market participants." Similarly, an SCI entity needs to provide such notice to the Commission only when the disruption "would have a material impact" on the entity's market or its participants. This reflects common-sense business realities where we normally would provide the Commission and our members with such information, and is

⁵ In fact, a third event produced a similar result. In August 2003 there was a blackout throughout much of New York City, including the Wall Street area. While ISE lost utility power, our generators continued to power our operations. Although utility power was restored before the next trading day, we would have been fully operational at either our primary or BC/DR site on a next-day basis even without utility power.

consistent with ARP's "system outage notification" requirement, which we believe has operated well.

There are similar common-sense limits regarding notices of system intrusions. While the SCI entity must report such intrusion immediately to the Commission, the Commission carefully limits the need for an SCI entity to notify its members of the event if the entity "determines that dissemination of such information would likely compromise the security of the SCI entity's [systems]." We believe this properly balances the need for providing the appropriate parties with information on the intrusion against the harm that could arise with premature notice to members of such an event.

In contrast, with system compliance issues, there is no "materiality" or "significant" reporting threshold, thus requiring reporting of all such events. Moreover, not only must the SCI entity report such events to the Commission, but it also must provide members with information regarding: the event; the types and number of members potentially affected by the event; and progress of corrective action. And this is not just a one-time notice requirement as the SCI entity must provide "regular updates" to its participants as new information becomes available.

We believe that this compliance reporting requirement would impose an unreasonable burden on SCI entities and would not provide the Commission and members with useful information. In this regard, the Commission defines a "systems compliance issue" to cover any event "that has caused an SCI system . . . to operate in a manner that does not comply with the federal securities laws and rules and regulations thereunder or the entity's rules or governing documents." In the increasingly complex world of electronic trading, there are complicated allocation algorithms and many different categories of customers (at least in the options market), that could lead to many technical compliance "issues" that have virtually no effect on members or the investment community.

We certainly agree that the Commission and members should know if an SCI entity's operations are materially out of compliance with its rules. Examples of such issues in the options market would be an exchange not providing priority to customer orders if the exchange's rules so provide. Similarly, it should apply if an exchange does not protect a significant set of orders against execution at prices inferior to away-market quotations. These situations are relatively rare and deserve wide-spread notice.

In contrast, most compliance "issues" relate to very technical matters and often may not have any real-world effect. Again, using the options market as an example, exchanges can have complicated execution algorithms that apply to both continuous trading and specialized auctions (such as facilitation trades), and all of which apply to both regular orders and complex orders. It is possible that when some combination of events occurs an exchange may find that a small portion of an order is misallocated. While software testing finds most of these issues before they can occur in a live production environment, it is not possible to test all conceivable trading scenarios. Indeed, an exchange may discover such an irregularity when doing regression testing of a new release, at which time it discovers a pre-existing coding error in its current production system. In such cases the exchange may never even know if the irregularity discovered in testing actually occurred in real-life trading.

As currently proposed, the Regulation likely would result in a flood of useless information to the Commission and our members that will make it nearly impossible for recipients to discern when there are compliance concerns that merit real attention. The Commission should more narrowly focus the dissemination requirement to system

compliance issues that have a material or significant effect on members. Even in those situations, the Commission should limit the requirement to providing notice to the Commission and only those members actually affected by the issue. Providing unnecessary notices of non-material issues serves no useful purpose and only serves to mask the significant issues that have a real effect on trading and the investing public.

III. Operational Aspects of the Regulation

A. Periodic Testing of Systems as Part of the Systems Compliance Safe Harbor

As discussed, the Regulation would require SCI entities to have policies and procedures reasonably designed to ensure that its SCI systems operate in the manner intended and in compliance with the federal securities laws and the entity's own rules. The Commission proposes a safe harbor regarding compliance with that requirement, which safe harbor includes certain testing requirements. Specifically, the safe harbor requires that the entity establish and maintain policies and procedures regarding testing of its SCI system and changes to such systems both prior to implementation and on a periodic basis following implementation.⁶

While we certainly endorse the need to test new systems and changes to such systems, we do not believe that the safe harbor should include the requirement that SCI entities conduct periodic testing of such systems after implementation absent system changes. Such a requirement would increase systems management costs without any significant benefit. SCI systems, particularly trading systems, consist of many components, most of which undergo changes infrequently. For those that do incur change, we perform testing prior to implementation in the production environment. Moreover, for any changed component, not only do we test the changes, but we also conduct regression testing to ensure that the changes did not introduce any undesired side-effects.

Since we conduct full regression testing on changes to SCI systems, re-executing these tests on a periodic basis will not produce any new results. Rather, the requirement for periodic testing will only result in additional costs for the SCI entities without any benefit. Requiring members to participate in such tests would further increase these costs. We thus recommend that the Commission replace the periodic testing requirement of the safe harbor with a requirement for regression testing of any changed component of an SCI system.

B. Definition of "SCI Security Systems"

The Regulation does not specifically define "SCI security systems" other than to state that these are systems that "share network resources" with SCI systems and that, if breached, would be reasonably likely to pose a security threat to SCI systems. The commentary gives very broad examples of such systems, including e-mail and intranet sites.⁷ We believe that the "share network resources" standard is very broad and could ensnare many peripheral systems in the definition. Because these systems are isolated from a security perspective from actual production or trading, we believe that the

⁶ Proposed Rule 1000(b)(2)(ii)(A)(1) and (2).

⁷ Specifically, the Release states that SCI security systems "may include systems pertaining to corporate operations (e.g., systems that support web-based services, administrative services, electronic filing, email capability and intranet sites, as well as financial and accounting systems) that are typically accessed by an array of users (e.g., employees or executives of the SCI entity) authorized to view non-public information." Release at 18099.

Commission should limit which systems are subject to the operative provision of the Regulation.

In this regard, we do note that Section (b)(1) of the Regulation states that the “policies and procedures” requirements apply to SCI security systems only “for purposes of security standards.” While we believe that this may be an appropriately limiting provision, we request that the Commission provide greater clarity on the extent to which it believes that SCI security systems isolated from production, such as e-mail and intranet sites, raise security issues that are within the scope of the Regulation.

C. System Change Notifications

The Regulation would require SCI entities to provide the Commission with notice of material system changes. This would codify the corresponding ARP requirement, which we believe has worked well. The proposed definition of “material system change” is similar to the current ARP definition and includes, among other things, a change that “materially affects the existing capacity” of an SCI system. Our sole concern regarding this notice requirement is the Commission’s commentary that “reconfigurations of systems that would cause a variance greater than five percent in throughput or storage” would be material.⁸

ISE routinely makes changes to its configurations to add capacity either for processing capability or storage, and we have never considered any increase in capacity to be a material change, let alone five percent. Such changes are “business as usual,” including the normal addition of servers or reconfigurations of existing systems. We believe that providing system change notifications of such regular activities is unnecessary and would be an undue burden. While a decrease in capacity may be noteworthy and reportable, we urge the Commission not to require reporting of routine activities, such as increases in capacity.

D. Disaster Recovery Testing

The Regulation would require SCI entities to conduct BC/DR tests at least once every 12 months. An SCI entity must coordinate these tests with other SCI entities on an industry- or sector-wide basis, and must designate members required to participate in such testing. It must designate those members whose participation “it deems necessary, for the maintenance of fair and orderly markets in the event of the activation of its business continuity and disaster recovery plans....” While we agree with requiring industry-wide BC/DR tests, we have concerns regarding two aspects of the proposal: the participation of members in such testing; and the possibility of requiring such testing in live production systems.

How best to include members in BC/DR testing is a complex issue, and SCI entities should have significant flexibility in this area. As currently proposed, the Regulation would require SCI entities to designate members required to participate in the testing and must notify the Commission of the identities of such members and the standards used in making the designations. While not specified in the Regulation itself, the commentary states that SCI entities that are SROs must file these standards as rule changes under section 19(b) of the Act.⁹ Although the Commission does not specify how many members would be required to participate in such tests, in its cost/benefit

⁸ *Id.* at 18105 and 18106.

⁹ *Id.* at 18126.

analysis the Commission assumes that 150 members or users of each SCI entity would be subject to this requirement.¹⁰

Although unstated in the Release, it is a given that requiring a member of an SCI entity to participate in BC/DR testing would require that member to connect to the SCI entity's BC/DR site. This could well pose a significant economic burden on the broker-dealer community. Indeed, we believe that the cost of such connections would be well more than the \$10,000 per connection that the Commission estimates.¹¹ We estimate that establishing and maintaining a connection with comparable trading capability and latency could cost a broker-dealer that co-locates at an SCI entity's data center between \$15,000 and \$20,000 monthly simply for the necessary communication lines.

In addition, such members would need additional hardware in order to establish an appropriate presence at the BC/DR site to ensure that they could trade in an efficient manner with low latency. We have regular discussions with our members on such requirements and costs and they uniformly believe that such costs would be very significant and would provide little benefit to the market. While we do not have exact hardware figures, we estimate that market makers could be required to spend up to \$500,000 for an appropriate hardware configuration at a DR/BC site.

Given the magnitude of these costs, complying with this requirement could cause broker-dealers to reduce the number of SCI entities through which they trade. Thus, a requirement intended to help ensure liquidity in the very rare situation of activating a BC/DR plan instead could cause a lessening of liquidity across the market in the 99+ percent of the time in which SCI entities are operating normally. This is especially true in our current market structure in which, as noted above, 14 SROs provide markets in equity securities and 11 SROs provide markets in listed options. Broker-dealers looking to control their costs may rationally decide to limit the number of markets on which they are members rather than establish relationships with all markets.

We recommend that the Commission adopt a narrower requirement regarding the inclusion of SCI entity members in BC/DR testing. Rather than those "necessary for maintenance of fair and orderly trading," we recommend that the standard be those members "critical to the operation of the SCI entity." As a practical example, at the ISE our focus would be on our members that provide continuous liquidity, our Primary Market Makers (of which we have seven). These members provide a base-line of liquidity for trading. In contrast, for us to provide "fair and orderly trading," we also may need members who access this liquidity, our Electronic Access Members ("EAMs"). Yet requiring some or all EAMs (of which we have approximately 145) more likely would lead to some EAMs dropping their membership on the ISE (or on other exchanges with similar requirements), harming liquidity during the vast majority of the time that we are engaging in normal operations.

The Commission also requests comment on the possibility of requiring BC/DR testing in a "live 'production' environment on a periodic basis."¹² For many of the reasons we have already discussed, we do not support such a requirement. BC/DR sites may not have the full capabilities of primary sites. Similarly, not all members will be connected to BC/DR site. For those that are connected, there may be limited functionality and almost certainly would be greater latency.

¹⁰ *Id.* at note 643.

¹¹ *Id.*

¹² *Id.* at 18113 and 18127.

A “live production” BC/DR test therefore would greatly compromise “normal” trading during this test period, while providing few if any incremental benefits over the current industry weekend tests. Moreover, it would be impossible to create a real-life disaster situation since the test would not be conducted during a true wide-spread disruption, in which transportation and other services likely would be unavailable. Thus, it would not be a true test. We believe the Commission should let the SCI entities and their members and other users develop their own BC/DR tests. Only if the Commission ultimately determines that such testing has not been adequate should the Commission intervene and consider mandating any particular type of test.

E. Commission Access to SCI Systems

The Regulation would require that SCI entities provide Commission staff “reasonable access to SCI systems and SCI security systems to allow Commission representatives to assess the SCI entity’s compliance” with the Regulation.¹³ The commentary in the Release states that such access could be “either remotely or on site.”¹⁴ In a footnote to that statement, the Commission implies that with remote access “Commission representatives could test an SCI entity’s firewalls and vulnerability to intrusion.”¹⁵

We believe it would be inappropriate to grant Commission staff remote access to our systems, on either a full-time or ad hoc basis. Providing any outside entity such access would greatly compromise our information technology security and would present a substantial risk to our production system. We perform our own vulnerability scans and have provided, and will continue to provide, the results of those scans to the Commission staff. That form of access is more than adequate access for the Commission to discharge its oversight responsibility with respect to SCI entities.

F. Prevailing Industry Standards

As discussed above, the Regulation requires SCI entities to maintain policies and procedures regarding the proper operation of their SCI systems, and includes a non-exclusive “safe harbor” with respect to that requirement. To fall within the safe harbor, the SCI entity must have policies and procedures consistent with industry standards “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.”¹⁶ The Commission provides a proposed preliminary list of such standards in Table A of the Release, and requests comment on whether such standards are “suitable” for the safe harbor.¹⁷

We believe that the standards listed in Table A are not the most current or appropriate standards. Many documents listed are nearly 10 years old and generally are inapposite. For example, for Systems Development Methodology the Commission lists a 2008 NIST document that only discusses security considerations and thus is not suitable for use as an overarching policy document. Also, for capacity planning, the Commission cites a 2004 Federal Financial Institutions Examination Council’s (“FFIEC”) document that describes an inspection process rather than overall capacity management.

¹³ Proposed Rule 1000(f).

¹⁴ Release at 18130.

¹⁵ *Id.* at note 264.

¹⁶ Rule 1000(b)(1)(ii).

¹⁷ Release at 18113.

We recommend that in adopting the Regulation the Commission specifically authorize SCI entities to establish an SCI standards committee charged with reviewing and recommending to the Commission specific documents for use in the safe harbor. We believe that would be the most efficient way for the Commission to receive input from the industry as to current industry practices and standards. For the most appropriate documents at this time, we recommend:

- For Application Controls, Information Security and Networking, and Physical Security domains: ISO 27001 is the most widely recognized information security framework.
- For Contingency Planning domain: NFPA-1600-Standard on Disaster/Emergency Management and Business Continuity Program, or BS 25999 Business Continuity Management Standard. These two standards have been adopted by the Department of Homeland Security.
- For the Audit domain, we recommend documents issued by either the Institute of Internal Auditors (“IIA”) or the Information Systems Audit and Control Association (“ISACA”), which are the globally recognized leaders. We believe these documents would be preferable to those of FFIEC.

IV. Economic Analysis

We appreciate the difficulty in estimating the costs the industry would incur in complying with major initiatives such as the Regulation. Thus, we believe that the Commission should have significant latitude in providing its statutorily-required cost/benefit analysis. Nevertheless, we believe that the Commission may well have begun that analysis from a faulty basis by assuming that SCI entities that have been subject to ARP have been in compliance with those voluntary standards. The Commission thus assumes that the cost of compliance with the Regulation would be the incremental costs above the ARP costs (either due to obligations above ARP standards or the imposition of those obligations on SCI entities not now subject to ARP).

By its very nature ARP is voluntary and there has been no regulatory obligation on SCI entities to comply with these requirements. Because there is no publicly-available information on voluntary compliance with ARP we cannot provide useful comments on whether this is the appropriate baseline for the Commission to use in determining the cost of the Regulation to the industry. Indeed, the only entity that has knowledge of such compliance is the Commission itself. Therefore, we believe that the Commission should calculate the actual cost based on its knowledge of the extent to which SCI entities currently subject to ARP are actually in compliance with that program, rather than simply assuming full compliance.

Regardless of the baseline the Commission uses, we believe that the Commission significantly underestimates the costs of compliance. Overall, the Commission estimates the costs of an SCI entity complying with the Regulation as between \$400,000 and \$3 million.¹⁸ As part of this cost, the Commission estimates that it would take SCI entities 625 hours to conduct a review of its compliance with the Regulation.¹⁹ In at least two areas we believe that this estimate is much too low.

¹⁸ *Id.* at 18171. In footnote 633 the Commission implies that this wide range is because a number of entities already are in, or are in the process of coming into, compliance with a variety of the Regulation’s requirements, including the next-day readiness requirements.

¹⁹ *Id.* at 18151.

First, our experience under ARP and with internal audit generally is that 625 hours significantly underestimates the amount of time it will take to conduct an SCI compliance review. We currently spend more time than that on ARP compliance matters alone, including our SSAE16 audit. We estimate that it will take us over 1200 total hours to comply with the Regulation.

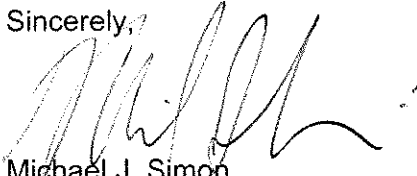
Second, we believe that the Commission has not appropriately considered the costs and benefits of maintaining geographically diverse data centers to meet the next-day readiness requirement. Other than the overall range of costs noted above, the Commission does not break out any specific costs of meeting this requirement. In fact, we believe that the cost of establishing and maintaining geographically diverse data centers alone will dwarf the estimated overall compliance costs of \$400,000 to \$3 million. We estimate that the incremental all-in, five-year costs to the ISE of relocating our BC/DR site a significant distance from the New York City area would cost us \$17 million over our current BC/DR plans.

We thus believe that the Commission must explore in much greater depth the costs of establishing and maintaining geographically diverse data centers at significant distances from each other if it believes that such data centers are necessary to meet the requirements of the Regulation. This would include the costs imposed both on SCI entities and on their members and other users. Furthermore, as discussed in detail above, the Commission must balance those costs against what we believe are the speculative benefits of such a requirement.

* * *

We again thank the Commission for the opportunity to comment on the Regulation. We look forward to working with the Commission in the coming months to help shape the proposal into a workable, cost-effective Regulation that will help address the very legitimate concerns giving rise to the proposal. If you have any comments on, or questions regarding our letter, please do not hesitate to contact us.

Sincerely,



Michael J. Simon
Secretary