Raymond Tamayo
Chief Information Officer

July 8, 2013

VIA ELECTRONIC MAIL

Elizabeth M. Murphy, Secretary
Securities and Exchange Commission
100 F Street NE.
Washington, DC 20549-1090

Re: File No. S7-01-13: Proposed Regulation Systems Compliance and Integrity

Dear Ms. Murphy:

The Options Clearing Corporation ("OCC") appreciates the opportunity to comment on the Commission's recent release proposing Regulation Systems Compliance and Integrity ("Regulation SCI").[1] Founded in 1973, OCC is currently the world's largest equity derivatives clearing organization. OCC clears security options, security futures and other securities contracts subject to the jurisdiction of the Securities and Exchange Commission ("SEC" or "Commission"), and commodity futures and commodity options subject to the jurisdiction of the Commodity Futures Trading Commission ("CFTC"). OCC will also begin clearing over-the-counter options on securities indices in the near future, pending final regulatory approvals. OCC is registered with the Commission as a clearing agency pursuant to Section 17A of the Securities Exchange Act of 1934 (the "Exchange Act")[2] and is registered with the CFTC as a derivatives clearing organization ("DCO") pursuant to Section 5b of the Commodity Exchange Act.[3] OCC clears all standardized options listed on the eleven U.S. national securities exchanges that trade options[4] and, in its capacity as a DCO, clears CFTC-regulated futures products for five

[1] Regulation Systems Compliance and Integrity, Release No. 34-69077, 78 Fed. Reg. 18084 (March 25, 2013) (the "Proposal" or "proposed Regulation SCI"). *See also* Regulation Systems Compliance and Integrity, Release No. 34-69606, 78 Fed. Reg. 30803 (May 23, 2013), in which the Commission extended the Proposal's comment period until July 8, 2013.

[2] 15 USC § 78q-1.

[3] 7 USC § 7a-1.

[4] OCC's participant options exchanges include: BATS Exchange, Inc.; BOX Options Exchange, LLC; C2 Options Exchange, Inc.; Chicago Board Options Exchange, Inc.; International Securities Exchange, LLC; Miami International Securities Exchange, LLC; NASDAQ OMX BX, Inc.; NASDAQ OMX PHLX, LLC; The NASDAQ Stock Market LLC; NYSE Arca, Inc.; and NYSE MKT, LLC.

6032 Innovation Way, Keller, TX 76244 817.562.3530 rtamayo@theocc.com www.theocc.com

U.S. futures exchanges.[5] OCC has also been designated by the Financial Stability Oversight Council as a systemically important financial market utility pursuant to Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Dodd-Frank Act").[6] Prior to enactment of the Dodd-Frank Act in July 2010, OCC was the only clearing organization that was dually registered as both an SEC-regulated clearing agency and a CFTC-regulated DCO. OCC has operated safely and effectively for 40 years—including through the market crises of 1987 and 2008—mitigating systemic risk associated with derivatives trading.

OCC supports the Commission in its efforts to increase safety and security in the national financial market system and appreciates this opportunity to comment on several aspects of proposed Regulation SCI that we believe should be improved or clarified before the Commission issues final rules. There are also aspects of the Proposal that will pose significant operational and administrative burdens on OCC and other market participants. We wish to ensure that the Commission has carefully considered whether all such burdens are warranted, given the benefits expected to be achieved by proposed Regulation SCI. Further, we believe certain aspects of the Proposal, while sensible in the abstract, may actually introduce new security threats to and increase the vulnerability of the core systems of entities subject to Regulation SCI. In certain instances, we believe the Commission will be able to achieve its goal of increasing safety and security in the national financial markets by modifying or eliminating aspects of the Proposal.

DISCUSSION

I. Implementation Timing of Regulation SCI

In the narrative accompanying the Proposal, the Commission indicated that the Proposal would formalize and expand many aspects of the Commission's Automation Review Policy ("ARP") statements, expand the scope of those statements to other systems and events and expand the scope of the ARP Inspection Program to other types of entities.[7] However, we believe that proposed Regulation SCI goes well beyond ARP and that it will pose substantial operational and administrative burdens and will take substantial time and expense to fully implement.

The Commission should not underestimate the resources that will be required in connection with new and changed systems and procedures designed to ensure compliance with Regulation SCI. Further, certain aspects of the Proposal will take much longer to implement than other aspects. For example, and as described in greater detail below, business continuity and end-to-end testing requirements, a two-hour recovery time objective and adopting policies

---

[5] OCC's participant futures exchanges include: CBOE Futures Exchange, LLC; ELX Futures L.P.; NASDAQ OMX Futures Exchange, Inc.; NYSE Liffe U.S. LLC; and OneChicago LLC.

[6] Public Law 111–203, 124 Stat. 1376 (July 21, 2010).

[7] Proposal at 18164.

and procedures in line with the proposed standards may each take longer to comply with than the other provisions of Regulation SCI.

Accordingly, we believe that, before issuing final rules, the Commission should consider the complexities associated with developing and implementing Regulation SCI and we therefore encourage the Commission to adopt a phased implementation schedule under which each SCI entity would, in successive order: (1) review its SCI systems risk-based assessment (as described below) with Commission staff; (2) review and update its policies and procedures to reasonably ensure compliance with Regulation SCI; (3) implement such policies and procedures; and (4) conduct an annual review. We believe that adopting such a phased implementation schedule will allow SCI entities to focus their efforts to achieve full compliance with Regulation SCI in a carefully considered manner and within a reasonable timeframe. To that end, OCC would gladly work with the Commission and industry groups in an effort to establish a detailed implementation schedule for Regulation SCI.

II. Definitions

We believe certain definitions in proposed Regulation SCI are overly broad or unclear as currently drafted:

SCI Systems and SCI Security Systems

The Proposal would define "SCI systems" as "all computer, network, electronic, technical, automated, or similar systems of, or operated by or on behalf of, an SCI entity, whether in production, development, or testing, that *directly support* trading, clearance and settlement, order routing, market data, regulation, or surveillance."[8] While we agree that the proposed definition of "SCI systems" may be appropriate for certain SCI entities, we are concerned that the proposed definition of SCI system is not appropriate for all SCI entities and we do not believe "SCI systems" can be defined via a prescriptive, one-size-fits-all approach. Further, considering the breadth of the listed functions of an SCI system, the use of the phrase "directly support" is both overly broad and vague and could be interpreted to include most, if not all, systems of an SCI entity.

We believe each SCI entity should be required to identify SCI system components and establish criticality ratings based on its own risk-based assessment, which would ultimately be used to determine which systems should be treated by the SCI entity as SCI systems. Further, as discussed in more detail below, we recommend that the Commission remove the definition of SCI security system and instead require SCI entities' risk-based assessments to consider any systems that share network resources with SCI systems that, if breached, would be reasonably likely to pose a security threat to SCI systems. This risk-based assessment would also provide a basis for determining materiality for purposes of Commission notification (as discussed in more detail below). Further, each SCI entity would review its risk-based assessment and discuss it

[8] Proposal at 18177-78.

with the Commission on an ongoing basis (*e.g.*, both following completion of the initial risk-based assessment and on an annual basis thereafter). If Commission staff were to believe an SCI entity's risk-based assessment disregarded systems that should be included in the definition, the Commission staff could consult with the SCI entity in an effort to ensure that those systems are included going forward.

We believe there is no uniform definition of SCI system that can be appropriately applied to every SCI entity without being greatly over-inclusive. Fortunately, this is not an instance in which regulatory flexibility in the Commission's approach to the definition of SCI system would promote an uncontrollable divergence of compliance outcomes or where thousands, or even tens of thousands, of market participants would be left to make their own determinations without Commission feedback. Instead, the number of SCI entities will be fairly limited and will be made up of a group of entities that, for the most part, already have extensive interactions with the Commission and its staff on an ongoing basis.

Should the Commission adopt such a risk-based framework, OCC would gladly work with the Commission and industry groups in an effort to establish criteria to be used by SCI entities in conducting their risk-based assessments for determining which systems to treat as SCI systems. We strongly believe that such a risk-based approach would focus the requirements of Regulation SCI on those systems that have the potential to actually disrupt market activities, and avoid drawing time and resources toward less vital systems. It would create a better framework to ensure that both the Commission and SCI entities consider current risk through ongoing risk analysis and discussion, thereby addressing threats common to the industry and unique to individual firms. It would also allow the scope of the rules to expand and contract over time in response to a changing risk landscape. This is essential because of the rapid pace of technological advancement, particularly in the financial markets. Given prior experience and the difficult regulatory realities faced by the Commission when implementing complex and technical rules such as Regulation SCI, we believe it is likely that whatever final rules the Commission promulgates will be on the books for many years to come. Adopting inflexible provisions (especially definitional provisions that determine the scope of the entire regulatory scheme) will not serve the Commission's interest in ensuring the technological integrity of the securities markets, nor will it serve the interests of SCI entities in meeting their obligations to their constituents.

Similarly, as described above, OCC believes a risk-based approach would address concerns expressed by the Commission with respect to the proposed definition of "SCI security systems." The proposed rules would define "SCI security systems" as "any systems that share network resources with SCI systems that, if breached, would be reasonably likely to pose a security threat to SCI systems."[9] We believe this definition is too broad and could capture certain systems of an SCI entity that are not appropriately treated as SCI security systems. Specifically, we believe including within the definition of SCI systems any systems other than those used by an SCI entity to enforce and monitor SCI system security policies would result in

[9] Proposal at 18177.

diversion of resources and focus toward less vital systems. Rather, OCC supports the approach suggested by the Commission whereby the defined term "SCI security systems" would be removed from the rules, but the final rules would clarify that, in adopting policies and procedures reasonably designed to ensure SCI systems have adequate levels of security, each SCI entity would need to assess security vulnerabilities created by other systems that share network resources with SCI systems and take appropriate steps to address those vulnerabilities.[10] Under such an approach, each SCI entity would still be required to take appropriate measures to ensure the security of its core systems but would do so holistically and in a more efficient and effective manner than if it were required to treat SCI security systems separate and apart from SCI systems.

The Proposal would include within the definition of SCI systems those systems that are part of an SCI entity's development or testing environments. OCC strongly believes that such systems should not be included within the definition of SCI systems. Development and testing environments are used for systems and application development for the specific purpose of identifying those systems and applications that are not operating as designed. Further, systems undergoing testing and development are operated in a protected environment, such that they do not have any significant impact on other SCI systems. If a systems issue were to arise within these environments, it would present little, if any, risk to an SCI entity's operations and would not pose any threat to the market in which an SCI entity operates. Accordingly, OCC believes that the cost to SCI entities associated with the inclusion of such systems within the definition of SCI systems would significantly outweigh any benefit the Commission would receive through notification of issues with such systems. We would agree, however, that to the extent a systems issue in a development and testing environment were to give rise to an issue affecting an SCI system, the requirements of Regulation SCI would apply.

SCI Events – Systems Disruptions

The Proposal would define an "SCI event" as "an event at an SCI entity that constitutes: (1) A systems disruption; (2) A systems compliance issue; or (3) A systems intrusion."[11] The Proposal would define a "systems disruption" as "an event in an SCI entity's SCI systems that results in: (1) A failure to maintain service level agreements or constraints; (2) A disruption of normal operations, including switchover to back-up equipment with near-term recovery of primary hardware unlikely; (3) A loss of use of any such system; (4) A loss of transaction or clearance and settlement data; (5) Significant back-ups or delays in processing; (6) A significant diminution of ability to disseminate timely and accurate market data; or (7) A queuing of data between system components or queuing of messages to or from customers of such duration that normal service delivery is affected."[12]

---

[10] Proposal at 18100.

[11] Proposal at 18177.

[12] Proposal at 18178. The Proposal indicates that a "systems disruption would be one that manifests itself as a problem measured by reference to one or more of [these] seven elements." Proposal at 18101.

In the narrative accompanying the Proposal, the Commission indicated that the proposed definition of "systems disruption" would be similar, but not identical, to the definition of "significant systems outage" under ARP.[13] However, as discussed in detail below, we believe the proposed definition of "systems disruption" is unclear and over-inclusive.

First, while we believe the seven types of events in the proposed definition of "systems disruption" are appropriate considerations in determining whether a systems disruption has occurred, we believe several of these types of events are in need of clarification. We also believe SCI entities should have more discretion and flexibility in determining whether the occurrence of any such event constitutes a systems disruption, with a proper view of the totality of the circumstances surrounding the event and its overall impact. As currently written, the Proposal appears to trigger an obligation to report any time one of the seven event types occurs, without regard to the materiality of the event to the operations of the SCI entity. The risk posed by a disruptive event varies greatly across SCI entities and across types of events. An event that raises serious operational issues for one SCI entity on one day may be a non-event to another SCI entity or on a different day. The occurrence of two different events that meet the defined categories may be of such vastly different levels of materiality that the two events should not be treated as both constituting "systems disruptions." For example, a disruption to systems access during critical processing windows is more significant than a disruption to systems access during non-critical times, which present little, if any, operational risk. OCC therefore encourages the Commission to include a materiality threshold such that only those systems disruptions that have a materially adverse impact on the SCI entity's ability to perform its core functions and critical operations are included within the definition of systems disruptions. By adopting such an approach, the Commission would appropriately recognize that each SCI entity is uniquely situated to determine, given the totality of the circumstances, whether the occurrence of an event in one of the seven categories is sufficiently material to constitute a systems disruption.

We also ask that the Commission clarify certain of the seven types of events described in the proposed definition. First, OCC believes that the inclusion of the failure to maintain service level agreements in the definition of a "systems disruption" is likely to have undesirable consequences. Specifically, in fear of being required to report minor breaches of service level agreements, SCI entities may forgo negotiating detailed and stringent service level agreements. We believe the cost of general and vague service level agreements significantly outweighs the

---

[13] *See* Securities Exchange Act Release No. 29185, 56 Fed. Reg. 22490 (May 9, 1991). In June 2001, staff from the Division of Market Regulation sent a letter to SROs and other participants in the ARP Inspection Program regarding Guidance for Systems Outage and System Change Notifications, advising them that the staff considers a "significant system outage" to include an outage that results in: (i) Failure to maintain service level agreements or constraints; (ii) disruption of normal operations, including switchover to back-up equipment with no possibility of near-term recovery of primary hardware; (iii) loss of use of any system; (iv) loss of transactions; (v) excessive back-ups or delays in processing; (vi) loss of ability to disseminate vital information; (vii) communication of an outage situation to other external entities; (viii) a report or referral of an event to the entity's board of directors or senior management; (ix) a serious threat to systems operations even though systems operations are not disrupted; or (x) a queuing of data between system components or queuing of messages to or from customers of such duration that a customer's normal service delivery is affected.

benefit, if any, of including a strict failure to maintain service level agreements in the definition of systems disruption. Rather, we believe only those most significant breaches of service level agreements which impede an SCI entity's ability to perform its core functions and critical operations should be included. Further, OCC appreciates the example the Commission provided in the narrative accompanying the Proposal regarding the types of service level agreements meant to be within the scope of a systems disruption. We believe the example is appropriately limited in its focus to service level agreements between an SCI entity and users of its SCI systems, and we believe the Commission appropriately excluded service level agreements between an SCI entity and its vendors.

Further, the inclusion of "a loss of use of any [SCI] system" is unclear. For example, certain of OCC's systems are configured for "high availability," where a system may "fail-over" to alternate servers without impacting the service itself. It is unclear from the Proposal whether such a "fail-over" would constitute a "loss of use of a system" when, in fact, the system is functioning as intended, with perhaps no or only minor impact on OCC's operations. This lack of clarity is likely to lead to interpretive differences and inconsistency among SCI entities. Another example may occur where an SCI entity has multiple vendors (*e.g.*, a primary and a secondary vendor) with communication lines connecting each vendor to multiple locations of the SCI entity's infrastructure. In such a configuration, a "disruption" of a communication line between the primary vendor and the SCI entity's infrastructure may result in a "fail-over" to its established back-up communication lines. Arguably, this does not actually result in a disruption of services and simply reflects the way the system was intended to function. In our opinion, it is unclear based on the proposed criteria whether such an event would constitute a loss of use of an SCI system.

In addition, OCC seeks clarity on the extent to which "a loss of transaction or clearance and settlement data" would constitute a systems disruption. For example, lost data is often retrievable though back-up systems. If an SCI entity were to immediately retrieve lost data, there would be no material disruption to an SCI system. We ask that the Commission clarify that only a loss of transaction or clearance and settlement data which is not immediately retrieved is included within the definition of a systems disruption.

The fifth and sixth event types of the proposed definition of "systems disruption" address system back-ups or delays and a diminution in ability to timely and accurately disseminate market data. While we do not disagree with the specific language used to describe the event types, we are concerned with the Commission's statements in the narrative accompanying the Proposal. In particular, the Commission indicated that these event types would be implicated if a customer or system-user were to complain or inquire about a slowdown or disruption.[14] While such a complaint or inquiry *may* be indicative of a systems disruption, it will not in all cases mean that such a disruption has, in fact, occurred. Instead, we believe the facts and circumstances should drive the determination of whether an event constitutes a systems disruption, and the fact that a customer or system-user placed a call or otherwise inquired about a

[14] Proposal at 18101.

slowdown would merely be one of the circumstances considered by the SCI entity. Accordingly, we request that the Commission clarify that customer or system-user complaints or inquiries with respect to back-ups or delays in processing *may be indicative* of a system disruption, depending on the circumstances, but will not constitute a *per se* systems disruption.

The seventh event type proposed to constitute a systems disruption is the queuing of data between system components or queuing of messages to or from customers of such duration that normal service delivery is affected. While OCC supports this part of the definition (which requires there to be an actual impact on service), we are concerned with aspects of the narrative accompanying the Proposal, in which the Commission states that "queuing of data . . . is often a warning signal of significant disruption."[15] By using the term "warning signal," the Commission seems to indicate that events that may be precursors to a systems disruption could themselves be considered systems disruptions. We believe the queuing of data or messages would only be a systems disruption if such queuing impacts critical operations, and we ask the Commission to clarify this in the final release.

III. Policies and Procedures

Written Policies and Procedures to Safeguard Capacity, Integrity, Resiliency, Availability and Security

The Proposal would require each SCI entity to "establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its SCI systems and, for purposes of security standards, SCI security 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."[16] Further, the Proposal would deem such policies and procedures to be "reasonably designed" if they are consistent with current "SCI industry standards." SCI industry standards, in turn, would then be required to be: (1) comprised of information technology practices that are *widely available for free* to information technology professionals in the financial sector; and (2) issued by an authoritative body that is a U.S. governmental entity or agency, an association of U.S. governmental entities or agencies, or a widely recognized organization.

In the narrative accompanying the Proposal, the Commission lists published standards that the Commission preliminarily identifies as "SCI industry standards."[17] A lack of agreed-upon standards has proven to be problematic with ARP, and OCC therefore appreciates the Commission's identification of an initial set of SCI industry standards that adopts a risk-based controls framework. In particular, we appreciate the identification of NIST 800-53 - NIST DRAFT Security and Privacy Controls for Federal Information Systems and Organizations

[15] Proposal at 18102.

[16] Proposed Rule 1000(b)(1).

[17] Proposal at 18111 (Table A – Publications Relating to Industry Standards in 9 Domains).

(Special Publication 800-53), which explicitly encompasses a "Build It Right" strategy designed "to give organizations near real-time information that is essential for senior leaders making ongoing *risk-based* decisions affecting their critical missions and business functions." The Proposal provides that compliance with current SCI standards is not meant to be the exclusive means through which an SCI entity would be permitted to comply.[18] However, we recommend that the Commission not limit the definition of SCI industry standards to only those standards that are *widely available* in the public domain and *free of charge*. We believe such limitations may encourage SCI entities to use standards that may be outdated when more suitable standards may be available and would be more appropriate. We encourage the Commission to modify its current list of SCI industry standards accordingly.[19]

Recovery Plans

Following a wide-scale disruption, the Proposal would require SCI entities to have business continuity and disaster recovery plans that ensure an SCI entity's resumption of clearance and settlement services within two hours.[20] While a two-hour recovery time objective is a laudable goal, and one that OCC and other SCI entities strive to achieve, in our view the current state of infrastructure and technology means that current guidelines remain appropriate to recover and resume clearing and settlement activities within the business day on which the disruption occurs, with the overall aspiration of achieving recovery and resumption within two hours.[21] If adopted, a strict recovery time objective of two hours may not be consistently achievable without sacrificing core functions and increasing the risk of errors and backlogs. Forcing SCI entities to achieve a two-hour recovery time could promote shortcuts, including potentially skipping vital operations checks and/or returning to operations at less than full capacity. We believe promoting these outcomes is ill-advised and could actually exacerbate disruptions.

---

[18] Proposed Rule 1000(b)(1)(ii)(B).

[19] We note, for example, that NFPA 1600 (Standard on Disaster/Emergency Management and Business Continuity Programs published by the National Fire Protection Association), ASIS Spc. 1-2009 (Organizational Resilience: Security, Preparedness, and Continuity Management Systems - Requirements with Guidance for Use published by the American Society for Industrial Security) and ISO 22301(Societal security -- Business continuity management systems --- Requirements published by the International Organization of Standardization) are all recommended by the U.S. Department of Homeland Security even though they would not meet the proposed requirement of being "widely available for free to information technology professionals in the financial sector." Each of these are examples of 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, but would not appear to be permissible due to the fact that each of these standards are available for a nominal fee.

[20] Proposed Rule 1000(b)(1)(i)(E).

[21] This would be consistent with the guidelines under which OCC currently operates. *See* Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System (available at http://www.occ.treas.gov/news-issuances/bulletins/2003/bulletin-2003-14a.pdf).

Furthermore, OCC currently practices its disaster recovery procedures on almost a monthly basis. While OCC strives to meet a two-hour recovery time objective in these drills, our experience has shown that it often takes longer than two hours to fully recover and conduct operational checks. We appreciate that SCI entities are vital nodes in the global financial system and should endeavor to return to full operating capacity as quickly as possible after a disruption of service. However, resumption of full SCI entity activities may take longer than two hours depending on the type, timing and magnitude of the disruption. Moreover, an SCI entity is in the best position to determine, under the circumstances, if it is prudent to wait until the next business day to resume full operations.

The Proposal would require SCI entities to conduct periodic capacity stress tests of systems to determine their ability to process transactions in an accurate, timely and efficient manner.[22] The Commission sought comment on the appropriateness of requiring that such tests be conducted at specific intervals.[23] OCC has a policy to perform capacity testing annually, and in some cases bi-annually; however, we strongly believe the need for capacity tests varies depending on the nature and type of SCI entity. The Commission should not prescribe specific intervals for systems capacity tests, but should instead allow SCI entities reasonable discretion in determining appropriate intervals.

Systems Compliance

The Proposal would require each SCI entity to "establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its SCI systems operate in the manner intended, including in a manner that complies with the federal securities laws and rules and regulations thereunder and the entity's rules and governing documents, as applicable."[24] The Commission has proposed safe harbors for SCI entities and their employees in response to this requirement. While we support the Commission's approach of providing SCI entities and their employees safe harbors under Regulation SCI, we are concerned that SCI entities and their employees would not have sufficient control to predictably fit within the safe harbors. Specifically, the safe harbors provide that SCI entities must establish and maintain policies and procedures reasonably designed to provide for testing prior to and after implementation, internal controls, ongoing monitoring, compliance assessments and review by regulatory personnel.[25] Further, SCI entities would need to establish and maintain a system for applying policies and procedures which would reasonably be expected to prevent and detect any violations of Regulation SCI.[26] The use of a reasonableness standard with respect to the design of systems

---

[22] Proposed Rule 1000(b)(1)(i)(B).

[23] Proposal at 18112.

[24] Proposal Rule 1000(b)(2).

[25] Proposed Rule 1000(b)(2)(ii)(A).

[26] Proposed Rule 1000(b)(2)(ii)(B).

and the discharge of duties under an SCI entity's policies and procedures would mean that an SCI entity and its employees would never know with certainty whether they meet the terms of the safe harbor. We therefore question the value of the safe harbors as proposed and request that the Commission consider including bright-line tests and minimum standards in the safe harbor provisions to better guide SCI entities and their employees in avoiding liability under Regulation SCI.

As part of the safe harbor for an SCI entity in proposed Rule 1000(b)(2)(ii)(A)(6), the SCI entity would be required to establish and maintain policies and procedures that are reasonably designed to provide for review by "regulatory personnel" of SCI systems design, changes, testing and controls. The Proposal does not provide guidance on the meaning of the term "regulatory personnel." We believe each SCI entity will have to consider idiosyncratic factors when determining whether particular personnel qualify as "regulatory personnel" and that each SCI entity should therefore have reasonable discretion in making this determination.

The safe harbor would also require an SCI entity's policies and procedures to be reasonably designed to provide for periodic testing of all SCI systems and any changes to such systems after their implementation. We believe the scope of this testing is unclear. For example, if an SCI entity implements a systems change for which notice was already provided to the Commission, it is unclear whether additional, post-implementation testing is required to ensure that the systems change is working properly. We request that the Commission provide further guidance with respect to this element of the safe harbor.

IV. Notification Requirements

General Matters

The Proposal would generally require an SCI entity to notify the Commission at the time responsible SCI personnel become aware of an SCI event and it is reasonably estimated that the SCI event would have a material impact on the operations of the SCI entity or market participants. We are concerned that the Commission has underestimated the time and resources required to responsibly prepare and send notifications to the Commission. In recognition of the more complete description below of what we believe to be the costs of compliance, we urge the Commission to provide an appropriate implementation period during which time SCI entities would be able to develop necessary processes to handle this expected increase in required notifications.

The Commission estimates that self-regulatory organizations ("SROs") participating in the ARP Inspection Program averaged six systems disruptions notices in 2011.[27] However, the Commission also estimates that under proposed Regulation SCI a typical SRO would have 40 immediate notification events and 65 written notification events. This projection represents a *ten-fold* increase over the current reporting levels under the ARP Inspection Program. The

[27] Proposal at 18148 - 49 (footnote 409).

Commission further estimates 20 hours per written notification (10 hours for attorney time and 10 hours for compliance manager time).[28]

In our opinion, however, this estimate fails to take into account technology staff and business operations personnel, who spend considerable time gathering facts and circumstances surrounding a systems issue. In many instances, this process requires input from several departments to assess the scope and impact of a given issue, determine the appropriate remedial steps to be taken, and consolidate this information for review by legal and compliance personnel for notification purposes. Understanding that the goal of Regulation SCI is to ensure resiliency and to protect the stability of the markets in the face of increased automation and the rapid pace of technological changes, we are concerned that the broad and ambiguous definitions contained throughout the Proposal will cause SCI entities to spend significant time and resources reporting on systems issues that are less critical and divert attention away from those issues that are indeed significant and pose significant risk to market participants.

The requirement to notify the Commission of an SCI event would be triggered by "responsible SCI personnel" becoming aware of an SCI event that is reasonably estimated to have a material impact on the operations of the SCI entity or market participants. In turn, the Proposal would define responsible SCI personnel to mean any personnel, whether an employee or agent, of an SCI entity having responsibility for a particular SCI system or SCI security system impacted by an SCI event.[29] OCC is concerned that by including technology personnel within the group of responsible SCI personnel, the Commission is focusing on the wrong group of individuals within an SCI entity. Technology personnel can include operators and other staff members who are not necessarily trained to assess the impact of a given systems issue and make determinations as to when an SCI event would reasonably be expected to have a material impact or otherwise interpret OCC's regulatory reporting obligations. OCC believes a more sensible approach is to establish a clear escalation procedure by which technology staff performs an assessment of a given systems problem and notifies IT management, who will coordinate with legal and/or compliance personnel to help determine whether a given problem requires notification to the Commission. OCC believes the definition of responsible SCI personnel should, at a minimum, be limited to officers of an SCI entity who are authorized to make these decisions.

SCI Events

The Proposal would require SCI entities to notify the Commission of system disruptions that the SCI entity reasonably believes would have a material impact on its operations or on market participants, any systems compliance issue, or any systems intrusion ("immediate notification SCI event").[30] We believe these requirements to notify the Commission of an SCI

[28] Proposal at 18149 (footnote 411).

[29] Proposal at 18177.

[30] Proposed Rule 1000(b)(4)(i).

event are ambiguous and the ambiguity may result in over-reporting of items that do not present actual risk to market participants. Without providing SCI entities reasonable discretion, such as through a more generally applicable reasonable belief standard, to determine whether a given event should be reported to the Commission, SCI entities, in an abundance of caution, may unnecessarily notify the Commission of events that may arguably meet the notification requirement but likely pose little, if any, risk to systems operations and market participants. Instead, OCC recommends that the Commission should adopt a risk-based approach to materiality in this context similar to the approach we are recommending with respect to the definition of SCI systems.

Under such a risk-based approach to Commission notification, each SCI event (*i.e.*, a systems disruption, systems compliance issue or systems intrusion) would undergo a risk-based assessment, and the obligation to notify the Commission, as well as members or participants in the case of dissemination SCI events, would be triggered based on the overall assessment of the impact of the event on the SCI entity and on market participants. For example, an SCI entity's notice requirements could be linked to the risk-profile of its SCI systems described above. Each SCI event would then be given a risk rating (*e.g.*, major, moderate or minor), such that SCI events that are given a "minor" risk rating (*e.g.*, a temporary interruption to an SCI entity without any material impact to members) would be deemed not to be material, and therefore not reportable; SCI events that are given a "major" risk rating (*e.g.*, events which have a market-wide impact) would be considered to be material, and therefore, reportable; and SCI events that are given a "moderate" risk rating (*e.g.*, disruptions to an individual SCI entity) could be material and would be subject to further assessment to determine an SCI entity's reporting obligations.

To supplement this risk-based notification approach, OCC recommends that the Commission require SCI entities to maintain a log of incidents, the corrective measures taken and the impact (even if minor) of such incidents. These records could be reviewed periodically by Commission staff. OCC believes adopting such a risk-based approach would minimize insignificant notifications to the Commission and help focus each SCI entity's notification obligations on those items that truly have the potential to impact the markets. In addition, we believe such a risk-based approach with respect to materiality should apply not only to systems disruptions but to systems compliance issues and systems intrusions as well.[31]

With respect to the timing for Commission notification, we believe the notification framework that is in place today under ARP is very effective and the notice requirements for SCI events in proposed Rule 1000(b)(4) should generally follow that same framework. Accordingly,

---

[31] We note, however, that if the Commission does not embrace a risk-based approach in its final regulations, we believe it would be appropriate for the Commission to include a materiality threshold within the definitions of systems compliance issue and systems intrusion. For example, the definition of a systems compliance issue could be limited to events that result in non-compliance and have a materially negative impact on the SCI entity's ability to perform its core functions. The definition of a systems intrusion could be limited to any unauthorized entry into the SCI systems or SCI security systems of an SCI entity, which the SCI entity reasonably believes may materially impact its ability to perform its core functions or critical operations.

for SCI events that could potentially have a market-wide impact or that the SCI entity reasonably believes could impact the SCI entity's core functions or critical operations, notifications should be required to be made immediately even outside of normal business hours. However, we believe the first step in the notification process for all other SCI events (those that do not present the risk of a material impact on the SCI entity itself or the larger securities market) should be notification to the Commission no later than the next business day.

In addition to the immediate notification requirement, the Proposal would require written notification to the Commission within 24 hours of responsible SCI personnel becoming aware of the SCI event.[32] While we understand the Commission's desire to obtain a written record of the SCI event relatively quickly following the occurrence of such an event, we recommend that the Commission require written notification to be made within 72 hours rather than 24 hours, with the understanding that periodic updates would be required as the investigation into an SCI event continued. A 72-hour notification rule would be more practical, particularly for those incidents that occur during non-business hours, including evenings, weekends, and holidays. Staff and resource availability may be limited during such times and access to vendors who may be needed for root-cause analysis may be limited as well. Further, we believe that the 72-hour timing is necessary because the thorough and precise level of preparation that is appropriate for a formal notification often requires marshalling information from across multiple business and technology units. We understand that the nature of certain SCI events may warrant prompt notification to the Commission, and we therefore agree with the requirement to provide periodic updates (even off-hours) as new information becomes available or as facts change in a way that impacts the initial risk-based assessment. However, OCC believes it is important that the reporting obligations established by Regulation SCI do not unwittingly interfere with an SCI entity's ability to investigate and take corrective action to resolve an SCI event. The time period and frequency of reporting should not be so onerous and prescriptive that resources are diverted from the investigation and resolution of the SCI event itself.

The Proposal would also require that corrective action be taken immediately upon responsible SCI personnel becoming aware of an SCI event.[33] We are concerned that this aspect of the Proposal fails to recognize the complexity inherent in determining an appropriate course of action upon the occurrence of an SCI event. Moreover, requiring immediate corrective action risks undermining the internal escalation policies and procedures of SCI entities, which if followed are likely to result in a complete and effective remedy and guard against hasty and ineffective corrective action by unqualified SCI personnel. As noted above, and in further considering the proper time frame in which SCI entities should be required to take corrective action, we ask the Commission to consider the interplay of this requirement with its proposed notification requirements.

---

[32] Proposed Rule 1000(b)(4)(ii).

[33] Proposed Rule 1000(b)(3).

Material Systems Changes

The Proposal would require SCI entities to notify the Commission of any planned *material* systems change.[34] Despite the proposed definition of "material systems change" and the Commission's statements in the narrative accompanying the Proposal, we believe the materiality threshold is unclear. This is in part due to the proposed definition's use of the term "material" to define itself (*e.g.*, a change to one or more SCI systems of an SCI entity that materially affects existing capacity, etc.) as well as a lack of detail accompanying the examples in the Proposal that frustrates practical application of the proposed rule. To clarify the trigger of the requirement, we recommend that SCI entities only be required to provide notification concerning systems changes that the SCI entity believes, in its reasonable discretion, pose a significant risk of increasing susceptibility to major outages or increasing risks to its core functions or critical operations.

In addition, we have several recommendations with respect to the proposed criteria SCI entities must consider in determining whether a given systems change is material. First, we note that we would not interpret system changes that upgrade or update existing technology but that largely perform the same function—albeit with improvements or enhancements—as being material systems changes. In addition, the Commission states in the narrative accompanying the Proposal that changes to external interfaces must be reported. We would not interpret this as requiring notice of alterations or modifications of screens from time-to-time without changing functionality. The Proposal also states that systems changes that "could require allocation or use of significant resources" would be material and therefore reportable. We request clarification of what is meant by this standard and its "significant resources" threshold. Absent clarification, we believe it is subject to widely varying interpretations and could result in an undesired level of variation in reporting practices. Lastly, the Commission states that changes that were, or would be, reported to an SCI entity's senior management would be material and therefore reportable. We do not believe that whether senior management is notified of a systems change is an appropriate litmus test for determining materiality in this context. Many non-material systems changes may be reported to the senior management of an SCI entity for a variety of business reasons that have little to do with the materiality of those changes from a risk or compliance perspective. Rather, we believe reporting systems changes to the Board of Directors, or to a similar governing body, is a more appropriate standard for determining materiality.

OCC is concerned with the Commission's estimation of time required to prepare notices with respect to systems changes. The Commission estimates two hours to prepare and submit each such notice. We believe this significantly underestimates the amount of time needed to prepare systems change notices. Describing technical changes involves the work of a tech-writer, who needs to collaborate with multiple groups on a project team, including the project manager, application development team and the testing and implementation teams. A large amount of information needs to be assembled from different groups and consolidated into a

[34] Proposed Rule 1000(b)(6)(i).

single report.[35] Unless the Commission intends for the scope of information provided within these notices to be limited to high-level descriptions and generally less detailed, our experience with the level of collaboration required across different business and technology groups within the organization is that preparation of these notices generally requires considerably more time than is estimated by the Commission. In light of the significant time and expense associated with preparing notices for systems changes, we believe it makes it all the more important to use a risk-based materiality threshold that would only require SCI entities to notify the Commission when an SCI entity reasonably believes that the systems change poses a significant risk of increasing susceptibility to major outages or increasing risks to data security.

The Proposal also would require each SCI entity to submit a report within 30 calendar days after the end of June and December of each year containing a summary description of the progress of any material systems change during the six-month period ending on June 30 or December 31, as the case may be, and the date, or expected date, of completion of implementation of such changes.[36] We request that the Commission clarify what is expected to be reported as part of the June and December reporting with respect to material systems changes. Under the Proposal, and as noted above, SCI entities would be required to provide to the Commission a system change notice at least 30 days prior to implementation of material systems changes. Given that notice would have already been provided, it is unclear to us what additional information is being contemplated by this requirement.

Dissemination of Information to Members and Participants

Proposed Rule 1000(b)(5) would require SCI entities to notify members or participants of certain information concerning a "dissemination SCI event." OCC believes some of the elements of the proposed requirement are vague or overly broad.

First, the definition of a dissemination SCI event includes a system disruption that results, or the SCI entity reasonably estimates would result, in significant harm or loss to market participants. In contrast, the threshold for Commission notification of a system disruption is when an SCI entity reasonably estimates that the systems disruption would have a material impact on: (1) an SCI entity's operations; or (2) market participants. Without a clearer standard of what is meant by "material impact" or "significant harm or loss," SCI entities would be left to perform an ad-hoc analysis on a case-by-case basis with respect to which system disruptions are required to be reported to the Commission and which are required to be disseminated to members or participants. Accordingly, we believe these differing standards are at a high risk of

---

[35] For example, we believe such report would include but not be limited to: (i) a high-level description of the functionality and configuration of the affected systems; (ii) a description of the systems development process; (iii) the relationship to other systems; (iv) changes to production schedules due to the planned system change; (v) any effects on capacity; (vi) a description of test results; (vii) a summary of test results; (viii) contingency protocols (*i.e.*, fall-back options and disaster recovery measures); (ix) vulnerability assessments and security measures; and (x) whether an SEC rule filing under Rule 19b-4 has been made in connection with the system change notification.

[36] Proposed Rule 1000(b)(8)(ii).

producing inconsistent application across SCI entities and even within a given SCI entity. Ambiguity surrounding the threshold standards under ARP has been a challenging issue, and we therefore request that the Commission clarify exactly what is meant by these competing standards. If no difference is intended, we strongly believe a consistent standard should be used.

Second, the Proposal would require *any* systems intrusion to be disseminated to members or participants, subject to limited exceptions where security may be further threatened. In the narrative accompanying the Proposal, the Commission noted that the introduction of malware would be a systems intrusion, provided that systems were actually breached. Under this requirement, even minor viruses that are managed and quarantined, and present no material risk, would require notification to the Commission as well as to members and participants. As the Commission proposed with respect to systems disruptions, we believe a "materiality" threshold should apply to systems intrusions before they are required to be reported to the Commission as well as to members or participants.

Lastly, we believe not all dissemination SCI events warrant dissemination to all members or participants of an SCI entity. Considering the breadth of the definition of "dissemination SCI event," many such events will only affect a limited subset of an SCI entity's members. We therefore believe SCI entities should be given a reasonable amount of discretion upon the occurrence of a dissemination SCI event to determine which members or participants should receive notification and the manner and timing in which notice is provided. In particular, the SCI entity should be able to limit the communication to those members and participants that are actually affected and to provide the communication on a confidential and secure basis when the SCI entity has reasonable certainty of the information that is required to be provided by proposed Rule 1000(b)(5).

IV. Business Continuity and Disaster Recovery

The Proposal would require SCI entities to mandate participation by designated members or participants in scheduled testing of the operation of their business continuity and disaster recovery plans, including backup systems, and to coordinate such testing with other SCI entities. As the Commission points out, the U.S. national securities exchanges closed for two business days in October 2012 in the wake of Superstorm Sandy, even though the securities industry's annual testing of how trading firms, market operators and their utilities could operate through an emergency using backup sites, backup communications and disaster recovery facilities occurred without significant incident just two days before the storm. We support the Commission's approach to mandate participation in testing by certain designated firms. Today, participation in such testing is optional, which leads to inconsistencies among members or participants. A mandatory system will help to eliminate those inconsistencies.

Despite our general support of mandatory participation by certain members or participants in scheduled functional and performance testing of SCI entities' business continuity plans, we take issue with the proposed logistics and implementation of such testing. We are concerned that requiring firms to perform industry–wide, end-to-end testing by processing transactions in their disaster recovery systems introduces risk to the markets in that testing in this

manner increases the chance that test transactions may be inadvertently introduced into production systems. OCC's systems, as well as the systems of many member firms, are configured to prevent test activity from being processed by production or disaster recovery systems. Removing these safeguards is likely to require significant resources and may introduce new risks and unintended consequences. We believe our views are consistent with those of many in the securities industry, and we believe the Commission should respond to these concerns by modifying proposed Rule 1000(b)(9) to provide more flexibility in its testing requirements.

In addition, the Proposal is unclear as to who would be responsible for planning and organizing the industry-wide testing mandated by proposed Rule 1000(b)(9)(ii). OCC believes that the logistics to orchestrate this type of industry-wide disaster recovery testing (*e.g.*, timing, scope, structure and governance) requires the leadership of a central entity with regulatory authority or an industry organization tasked with this responsibility by the industry regulatory authorities. Further, there are concerns about the size and scope associated with performing industry-wide, end-to-end testing. Industry-wide tests are generally conducted over weekends when markets are closed, and there are legitimate concerns as to whether such complex testing scenarios can be conducted over the course of one weekend. Individual firms, including OCC, engage in ongoing testing of their systems' components on a regular basis, including regular connectivity tests.

If the Commission chooses to include in the final regulation a requirement for end-to-end testing, OCC would encourage the Commission to adopt a phased-in approach, where SCI entities could conduct testing of specific SCI systems over time, rather than be required to conduct a full end-to-end test, which cannot be done within a reasonable timeframe.

Finally, OCC is also concerned that under the Proposal an organization that may be a member or participant of multiple SCI entities could be subjected to several individual tests required by each SCI entity for which it is a member or participant. Without clearly defined industry level coordination, such organizations could face an exceedingly burdensome set of testing requirements imposed by each SCI entity for which it is a member or participant.

V. Review of Systems

The Proposal would require each SCI entity to conduct a review of its compliance with Regulation SCI not less than once each calendar year and submit a report of the review to senior management of the SCI entity for review no more than 30 days after completion.[37] Proposed Rule 1000(a) would define the term "SCI review" to mean a review, following established procedures and standards, that is performed by objective personnel having appropriate experience in conducting reviews of SCI systems and SCI security systems, and which review contains: (1) a risk-based assessment with respect to such systems of the SCI entity; and (2) an assessment of internal control design and effectiveness to include logical and physical security

[37] Proposed Rule 1000(b)(7).

controls, development processes and information technology governance, consistent with industry standards.[38] However, in the narrative accompanying the Proposal, the Commission stated that the proposed requirement would "formalize a practice in place under the current ARP Inspection Program in which SROs conduct annual systems reviews following established audit procedures and standards that result in the presentation of a report to senior SRO management on the recommendations and conclusions of the review."[39]

OCC requests that the Commission clarify the requirements with respect to annual reporting. For example, as part of its ongoing participation in ARP, OCC performs annual audits of technology systems associated with the clearance and settlement processes. These audits are designed to provide for management response, and the audit reports are provided to Commission ARP staff on a regular basis. We believe these existing assessment practices developed in connection with ARP are consistent with the proposed SCI review requirement. If, and to the extent, the Commission intends to require additional reporting beyond the internal audit reports described above, we ask the Commission to clarify such additional requirements. We also note that the ARP Inspection Program involves an annual on-site inspection by the Commission, but proposed Regulation SCI does not include this requirement. To the extent the proposed SCI review process is intended to eliminate the Commission's annual on-site inspection, we request that the Commission provide clarification in this respect.

There are also several points of modification we believe would enhance the proposed SCI review requirement. For example, proposed Rule 1000(b)(7) does not recognize that reasonable risk assessments may provide that it would be appropriate to review certain areas less frequently than annually. In fact, that may be the case because those areas inherently present limited risks or because of the high quality of the control environment. Hard wiring a static, annual requirement increases the likelihood that SCI entities would unnecessarily dedicate significant audit resources to such areas of lower risk. To ensure that SCI resources are utilized efficiently and effectively, OCC recommends that rotational risk-based internal audit reports should be accepted instead of requiring a consolidated annual report each calendar year.

In the interest of efficiency, OCC also recommends that the distribution cycle within proposed Rule 1000(b)(8)(i) be modified so that audit reports may be bundled and distributed to the Commission on a regular basis (*i.e.*, semi-annually or quarterly). Currently, the Proposal would require delivery to the Commission on a report-by-report basis.

OCC and other registered clearing agencies that fall within the proposed definition of SCI entity follow the SEC staff's guidelines for compliance with Section 17A of the Exchange Act in the Announcement of Standards for the Registration of Clearing Agencies.[40] Section IV.G. of

---

[38] Proposed Rule 1000(a).

[39] Proposal at 18123.

[40] *See* Securities Exchange Act Release No. 16900, 45 Fed. Reg. 41920 (June 23, 1980).

that guidance, titled Internal Accounting Control Reports, calls for the board of directors of a clearing agency to obtain an annual opinion report on internal controls from an independent public accountant. The work for clearing agencies to support that annual review overlaps with the proposed requirement in Rule 1000(b)(7) concerning an assessment of internal control design and effectiveness. To limit redundancies with respect to the Commission's expectations for clearing agencies, OCC believes the Commission should consider further coordination on these points.

VI. Access to Systems

While we understand the Commission's desire to have access to SCI entities' SCI systems and SCI security systems to ensure that Regulation SCI is properly implemented, we believe proposed Rule 1000(f) is unnecessarily and disruptively broad and introduces a new source of risk to SCI entities. Proposed Rule 1000(f) would require SCI entities to provide Commission representatives with reasonable access to their SCI systems and SCI security systems either remotely or on-site. For example, under the Proposal, Commission representatives would be given access to an SCI entity's SCI systems and SCI security systems in order to test an SCI entity's firewalls and vulnerability to intrusions. The Commission requested comment as to whether certain restrictions should be placed on the proposed access that would still allow the Commission and its representatives to evaluate an SCI entity's systems.

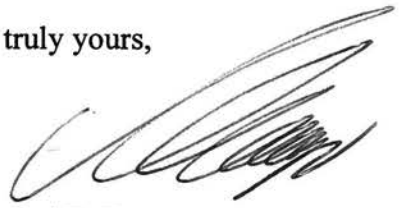
OCC believes the proposed access grants the Commission unnecessarily broad access to SCI systems and SCI security systems, especially for purposes of testing security. Vulnerability and intrusion testing requires highly-skilled staff members who are intimately familiar with ongoing production processing efforts. Instead, SCI entities could provide Commission staff with information sufficient to provide an assessment of the configuration and vulnerability status of the SCI systems. This information could be provided during the course of regularly scheduled examinations and supplemented as requested by the Commission. Alternatively, we would recommend that the Commission adopt a practice currently supported by OCC and the SEC's ARP staff, whereby testing is done on-site, performed by OCC staff and witnessed by ARP staff. Under this approach, access to an SCI entity's systems would be coordinated between the SCI entity's staff and the Commission to determine the specific tools, policies and configuration of such access. Further, the specific systems to be accessed should also be discussed in advance as well as the timing of access to such systems so that the risk of any systems disruptions is minimized. Either or both of these recommendations would create a clearly defined, efficient way for Commission staff to access information in order to perform their supervisory function and would ensure that access to these systems does not compromise the underlying goal of Regulation SCI to maintain integrity of SCI systems.

As a more global point in connection with proposed Rule 1000(f), we believe the Commission should bear in mind that access to such highly sensitive environments of SCI entities carries a duty of care commensurate with the sensitivity of the access and information involved. Accordingly, the resources and capacity of the Commission should be scaled to the level of access the Commission requires. We believe this point is also important to ensure high

quality interactions between Commission staff and personnel of SCI entities who are involved with SCI systems and SCI security systems.

OCC appreciates the opportunity to comment on the Commission's Proposal. We would be pleased to provide the Commission with any additional information or analysis that might be useful in determining the final form of Regulation SCI.

Very truly yours,



Raymond T. Tamayo

cc: James E. Brown, The Options Clearing Corporation
Jean M. Cawley, The Options Clearing Corporation
Daniel R. DeWaal, The Options Clearing Corporation
James R. McDaniel, Sidley Austin LLP
Nathan A. Howell, Sidley Austin LLP