September 25, 2013

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

RE: File No. S7-01-13; Regulation Systems Compliance and Integrity

Dear Ms. Murphy:

Direct Edge Holdings ("Direct Edge")[1] appreciates the opportunity to offer its views to the Securities and Exchange Commission ("Commission") regarding proposed Regulation SCI under the Securities Exchange Act of 1934 ("Exchange Act"), which is commonly known as "Reg SCI".[2]

I. Executive Summary

Direct Edge unequivocally supports the concept of Reg SCI as a mechanism to improve risk-management systems in our nation's financial markets and improve investor confidence therein. Formalizing and broadening Commission oversight of the key technological and operational underpinnings of market infrastructure can help maintain industry focus and prioritization in these areas and give the investing public greater faith in the existence and maintenance of high standards. In an era where technology is the foundation that supports all aspects of market operation, investor faith in our industry's ability to appropriately mitigate related risks is essential.

To achieve these objectives successfully and efficiently, Direct Edge believes that the final form that Reg SCI takes should be with the following principles in mind:

1. Have a narrow, risk-based focus on industry participants that are essential to continuous market-wide operation;

2. Design Reg SCI to reflect a realization that it serves as a framework for risk mitigation, as opposed to risk elimination;

3. Recognize that the regulated participant is the best (and in many ways only) entity suitably equipped with the knowledge and capabilities to manage its own technological and operational risks;

4. Realize that Reg SCI would only supplement commercial incentives to manage such risks, and would not be the sole (or even primary) driver of an affected entities' risk-management systems;

[1] Direct Edge is one of the leading stock exchange operators in the United States and globally. More information about Direct Edge is available at http://www.directedge.com.

[2] See 69077 (March 8, 2013), 78 FR 18083 (March 25, 2013) ("Proposing Release").

5. Acknowledge that there are multiple ways to achieve the same risk-management objectives, and any "hard coded" solutions are likely to become obsolete very quickly; and

6. Implement Reg SCI in a collaborative manner with affected industry participants, rather than in a manner structured to retro-actively hold regulated entities and their personnel accountable when risk events inevitably occur.

Direct Edge's comments are intended to bring the current proposal into greater alignment with these principles. We offer them because we believe that if structured and implemented in this manner, Reg SCI has the potential to be a highly constructive piece of regulation. But this opportunity could be lost if the final rules are over-broad in their scope, overly burdensome in their requirements, or overly critical in their application.

II. Comments on Proposed Rule Scope & Definitions

a. "SCI Entity" Definition

As discussed above, Direct Edge favors a narrow scope to Reg SCI such that only firms that are truly essential to continuous market-wide operation are classified as "SCI Entities". This should clearly include SEC-licensed exchanges, securities information processors under approved National Market System plans for market data,[3] and clearance and settlement systems. Beyond this limited universe, however, the purpose of Reg SCI would appear to morph beyond ensuring the systemic operational integrity of our nation's critical market infrastructure into something very different, and arguably much less beneficial relative to the costs.

This nexus between scope and regulatory intent is no more glaring than in the proposed definition's inclusion of small alternative trading systems ("ATSs"). Direct Edge believes that the applicability of Reg SCI to ATSs should be considerably reduced, relying perhaps on the existing twenty-percent threshold already established within Reg ATS.[4] This pre-existing standard – or some equivalent thereof – would be a more appropriate benchmark for bringing a non-exchange trading system within the ambit of Reg SCI regulation, with the significant compliance costs and customer testing obligations that would come therewith.

b. "SCI System" and "SCI Security System" Definitions

Direct Edge believes the Commission should exclude test systems from the definition of "SCI System" because of inherent conflicts their inclusion would create. While Direct Edge strongly believes in a testing infrastructure that closely mirrors production systems, the nature and purpose of such test environments would make compliance with Reg SCI difficult at best – and impossible at worst. AN SCI Entity would in theory need to have policies and procedures designed to test changes that are to be made to a test system for compliance with its obligations under Proposed Rule 1000(b)(2), and periodically "test the test system" to see if it was operating in the manner "intended". The whole purpose of test systems is to understand – and at some times to force – aberrant behavior or capacity issues. To bring such test systems within the "SCI System" definition, and the requirements that would flow from such a classification, would potentially eviscerate their very purpose.

---

[3] The Commission should clarify that, with respect to a Processor that meets the definition of an SCI Entity in another capacity (such as an exchange), said Processor needs to comply with Reg SCI independently or, in the alternative, any overlap should be fully disclosed to the Commission and Plan participants as part of the Processor's obligations under Proposed Rule 1000(b)(7).

[4] *See generally* SEC Regulation ATS, Rule 301(b)(6).

Regarding the "SCI Security System" definition, Direct Edge suggests a narrowing of the definition that specifically excludes any system that is: (a) logically separated from SCI Systems (so long as that separation is routinely monitored and has appropriate risk controls in place); and (b) "air gapped" (*i.e.*, has no point of entry from) the public Internet. Limiting the definition would significantly reduce the scope, and minimize any unintended consequences, with little to no incremental risk. As written, the current definition is so broad that could be read literally to include even the systems of an exchange's members, given the ability of a member to enter orders that could compromise capacity.

c. "SCI Events" and "Dissemination SCI Events" Definitions

Direct Edge believes the Commission should consider modification of the scope of the definitions of "SCI Events" and "Dissemination SCI Events." In particular, SCI Events should exclude seamless failover to a back-up system absent an impact on normal operations. One of the underlying purposes of Reg SCI is to promote resiliency of key market infrastructure while maintaining fair and orderly markets. If failover occurs without disrupting said markets, the value of classifying such a failover as an SCI Event is questionable.

Regarding the "Dissemination SCI Events" definition, Direct Edge strongly suggests the Commission consider the potential national security implications of mandating all system intrusions be disclosed to the public. There is a risk-based reluctance to share cyber vulnerability information publicly because any system vulnerabilities comprise highly-sensitive information, the public disclosure of which could actually invite additional cyber-attacks. Information shared with the government could potentially be released through government employee error or as the result of a Freedom of Information Act ("FOIA") request.[5]

Other government agencies have acknowledged the validity of these concerns and put statutory protections in place to address them. For example, under Section 211 of the Homeland Security Act, mechanisms exist for the protection of sensitive cyber-security information shared with the Department of Homeland Security ("DHS"), whereby information cannot be disclosed to any other part of the government or under the authority of a FOIA request, except under very limited circumstances. Currently, DHS signs Cooperative Research and Development Agreements ("CRADAs") with companies that are willing to share information with the government, thereby invoking the protections of Section 211. The Commission should consider a similar framework for reporting of System Intrusions to the Commission, and require public disclosure only in connection with instances where there is a risk of significant harm to the SCI Entity's customers, to ensure such sensitive information does not fall into the wrong hands.

d. "Material System Change" Definition

Direct Edge believes the definition as drafted, given the requirements that would be triggered thereby under Proposed Rule 1000(b)(6), are overly broad and rife with potential unintended consequences. While implying some notion of risk-adjusted analysis, the stated definition and related examples contain many absolute determinations that would trigger compliance requirements. Routine capacity upgrades, server and network hardware upgrades, any change to a Reg SCI system discussed with senior management, any change that "could" increase risks to data security, all could be used to classify the most routine business operations as

[5] Direct Edge would support limited broader disclosure of such intrusions to law enforcement agencies in a systemized way, such as through the Federal Bureau of Investigation's iGuardian portal launched in August 2013. *See* http://www.fbi.gov/news/podcasts/thisweek/iguardian.mp3/view.

"Material System Changes". While these concerns would be mitigated were the Commission to eliminate Proposed Rule 1000(b)(6) from the proposal,[6] at a minimum we believe the Commission should consider modifying its guidance on what constitutes "materiality" and instead rely on a risk-weighted determination made by the relevant SCI Entity.

III. Comments on Proposed Rules

a. Proposed Rule 1000(b)(1) – Policies and Procedures

Direct Edge is generally supportive of the premise of Proposed Rule 1000(b)(1), in that they include elements of a risk-management program that any critical infrastructure provider in our securities markets should already have in place. While the complex nature of modern technology and market operation means that having a malfunction is not *per se* a sign that a firm's control environment was not reasonably designed and adhered to, setting a baseline of expectations in this area can help promote the goals of best practices and sustained investor confidence that Direct Edge feels is Reg SCI's greatest potential value.

With that underlying support in mind, Direct Edge would offer the following comments::

- There is little discussion of the standard inherent in the rule "to maintain… operational capability and promote the maintenance of fair and orderly markets." There is an implication that adherence to industry standard procedures would comply with these requirements, but that alone does not sufficiently explain the standard to which SCI Entities will be held. In particular, the standard of "maintaining operational capability" is easier to grasp in the context of Reg SCI, in that is an introspective standard relevant to the applicable SCI Entity. The standard of "promoting the maintenance of fair and orderly markets," however, implies some incremental responsibility to the collective market that is hard to quantify or comply with in this context. As SEC oversight of market-participant technology moves from voluntary programs like ARP to mandatory requirements with enforcement implications, the SEC should carefully consider the precise standard to which SCI Entities would be held, what it means, and how firms should anticipate SEC expectations both before implementing compliance systems and when future difficulties are revealed.

- The proposed approach to business continuity planning ("BCP") and disaster recovery ("DR") requires significant re-evaluation. Again, Direct Edge fully supports the notion of robust and continual BCP and DR capabilities – and invests significant resources in these areas. The precise language of Proposed Rule 1000(b)(1)(i)(E), however, has significant deficiencies. It appears that proposed rule has been influenced by the events of Superstorm Sandy,[7] and a perception that the decision to refrain from trading while the storm abated was a sign of BCP and DR weakness. BCP standards – such as "ensure next-business day resumption" - that would apply in <u>all</u> circumstances without any acknowledgement of the infinite permutations of potential BCP and DR event scenarios, many of which cannot be anticipated in advance like a hurricane or a snow storm. It also focuses exclusively on wide-scale disruptions, when many BCP and DR events are local in nature. These concerns are augmented by language that blurs the fact that BCP and DR planning are related, but still independent disciplines. This is most glaring when considering an SCI Entity's most

[6] *See* Section III.f *infra.*
[7] *See* Proposing Release, at 27-28.

These concerns are augmented by language that blurs the fact that BCP and DR planning are related, but still independent disciplines. This is most glaring when considering an SCI Entity's most important asset – its people. BCP planning includes an assessment of critical personnel necessary to operate required systems and implement business processes, and efforts to ensure their general availability in disruptive scenarios, and maintain their ability to perform their expected responsibilities. Part of this planning is to leverage DR capabilities so that personnel can utilize them in appropriate scenarios. For many prospective SCI Entities, there are limited or no "DR" personnel (*i.e.*, alternative personnel that provide resiliency when existing personnel are not available due to a wide-scale disruption). Accordingly, in an unanticipated wide-scale disruption (such as a terrorist attack or earthquake) it is a real possibility that an SCI Entity's personnel, who are not geographically diverse at that time, would have their transportation and telecommunications capabilities significantly degraded, impacting their ability to physically get to, "tele-commute" to, or otherwise utilize even geographically-diverse DR facilities. These effects could impact the ability of an SCI Entity to resume trading operations the next business day, especially if a disruption occurred in the evening.

As written, Proposed Rule 1000(b)(1)(i)(E) and related commentary suggests that an SCI Entity would be held liable in such a circumstance for a violation of the rule, in that all elements of its BCP plan were not "sufficiently geographically diverse". Absent a continual maintenance of sufficiently-skilled employees across multiple geographic locations, compliance would likely be impossible. While one could argue these regulations would be applied and enforced on an *ad hoc* basis by regulators, such an assumption is more comforting in the context of a voluntary program like ARP as opposed to the mandatory regulation of Reg SCI.

Accordingly, Direct Edge believes that Proposed Rule 1000(b)(1)(i)(E) should be modified to require "comprehensive business continuity and disaster recovery plans with recovery time objectives of the next business day for trading and two hours for clearance and settlement." Accompanying guidance can continue to emphasize the belief that geographic diversity of physical facilities would be an expected component of any such plan. This more open-architecture language would be more reflective of the nature or BCP and DR best practices and more in line with the goal of risk mitigation, as opposed to risk elimination.

- The requirement of Proposed Rule 1000(b)(1)(i)(F) for "standards that result in such systems being designed, developed, tested, maintained, operated, and surveilled in a manner that facilitates the successful collection, processing and dissemination of market data" appears redundant given the other standards of the rule. Direct Edge would assume such requirements are a sub-set of the general requirement to "maintain… operational capability," and thus we question the additive value of an additional explicit requirement. While believing that market-data systems are critical to an SCI Entity's operation, Direct Edge believes this requirement should be eliminated and effectively "folded in" to other obligations.

b. Proposed Rule 1000(b)(2) – Policies and Procedures – System Compliance

Direct Edge is again generally supportive of the premise of Proposed Rule 1000(b)(2), in that it appropriately stresses the importance of a governance-based framework around the operation of essential IT assets. As constructed, Proposed Rule 1000(b)(2)'s implementation reality would largely focus on compliance with the "safe harbor" requirements detailed in Proposed Rule 1000(b)(2)(ii). With our general support for the Proposed Rule in mind, Direct Edge offers the following comments to make the safe harbor more workable in conjunction with other aspects of Reg SCI, and more consistent with the principles we believe should govern its adoption as outlined above:

- The testing requirements of sub-section (A) of the safe harbor are overly broad and potentially incompatible with both the notion of disciplined change management and the proposed definition of "SCI System." By requiring the testing of "any changes to [SCI] [S]ystems prior to implementation" and "[p]eriodic testing of all such systems and any changes to such systems after their implementation," the safe harbor would potentially drive SCI Entities to take a narrow view of what constitutes a change (a term not defined in the Proposing Release). Direct Edge believes that change management works best when the notion of a change is defined more broadly.[8] Under the proposed approach, any opening of a customer port, the removal of access rights from a departing employee, even the previously unscheduled closing of the market for the death of a U.S. president all involve "changes" to SCI Systems that need to be tracked, approved and catalogued within the construct of an enterprise-wide change management system. But they cannot all be tested, either prior to or after implementation, without an extraordinary amount of redundancy and bureaucracy, if at all.

  Direct Edge believes it would be more appropriate to modify sub-section (A)(1) of the safe harbor to require "Appropriate testing of such systems and changes to such systems prior to their implementation," and to modify sub-section (A)(2) to require "Appropriate testing of such systems and changes to such systems after their implementation." Removal of absolutist words like "any" and "all" would foster better change-management practices in Direct Edge's view, and potentially ease compliance burdens significantly.

- The proposed safe harbor for individuals, and the implication of potential individual liability created thereby, may have the unintended consequence of limiting the ability of SCI Entities to hire the best available talent in information technology, risk-management and compliance disciplines. By its very inclusion, the safe harbor appears to suggest a potential Commission focus on pursuing enforcement actions against individual employees for the IT failures of their institutions. Standards such as "do not have reasonable cause to believe" would not even hinge on actual knowledge, but what knowledge a "reasonable person" would or should have had. Accordingly, employees would bear a higher level of potential individual liability working at an SCI Entity than a firm outside the scope of the rule. Given the importance of human capital in any risk-management system, Direct Edge questions the focus on individual employees and respectfully suggests that absent an intentional act of willful misconduct, individuals should not be subject to Reg SCI liability.

[8] *See* ITIL® Glossary and Abbreviations (English Language version), *available at* www.itil-officialsite.com/InternationalActivities/TranslatedGlossaries.aspx (defining a "change" as "the addition, modification or removal of anything that could have an effect on IT services. The scope should include changes to all architectures, processes, tools, metrics and documentation, as well as changes to IT services and other configuration items.)

c. Proposed Rule 1000(b)(3) – Corrective Action

Direct Edge is again generally supportive of the premise of Proposed Rule 1000(b)(3), in that it a reflection of the responsibility of national securities exchanges and other self-regulatory organizations to promote fair and orderly markets under the Exchange Act. This support notwithstanding, Direct Edge believes the language of the proposed rule needs significant revision on the following grounds:

- The language is unrealistic and over-reaching in nature given the permutations of what an "SCI Event" might be, and the broad definitions and requirements. Requiring any responsible SCI personnel to take appropriate corrective action "upon becoming aware" of an SCI Event fails to acknowledge the difference between understanding that an event is in progress and knowledge of the root cause of said event (and potentially the appropriate corrective action that should be taken). It is also aggressive to presume that one individual's knowledge should prompt an immediate response by the SCI Entity at large, in certain circumstances. In addition, the standard that would require SCI Entities to "mitigat[e] potential harm to investors" – while noble in its intent – is extremely vague from the perspective of an enforceable Commission rule.

- Direct Edge respectfully proposes alternative language that would be cross-referenced with Rules 1000(b)(1) and 1000(b)(2). In particular, the paragraph could be revised to state:

  "When any responsible personnel of an SCI Entity become aware of the potential existence of an SCI Event, they shall begin to take appropriate corrective action including, at a minimum, invoking policies and procedures promulgated in compliance with Rules 1000(b)(1) and 1000(b)(2) to communicate the potential existence of an SCI Event among responsible personnel, diagnosing the scope of the potential SCI Event and its root cause, mitigating where practicable potential harm to investors and market integrity resulting from the SCI Event, devoting adequate resources to remedy the SCI Event as soon as reasonably practicable and notifying members or customers, as applicable, where required pursuant to Rule 1000(b)(5). Notwithstanding anything to the contrary, nothing in this Rule 1000(b)(3) shall require an SCI Entity to deviate from the policies and procedures promulgated under Rules 1000(b)(1) or 1000(b)(2)."

As revised above, Proposed Rule 1000(b)(3) would complement the other incident-related provisions of Reg SCI, rather than potentially conflict with them.

d. Proposed Rule 1000(b)(4) – Commission Notification

Effective and thorough incident-related communication with the Commission is an objective that Direct Edge whole-heartedly agrees with. In that spirit, we offer the following observations and suggestions:

- We question the feasibility, need and potential impact of the requirement of Proposed Rule 1000(b)(4)(iv)(C) that an SCI Entity provide a copy of "any information disseminated to date regarding the SCI Event to its members or participants." When an exchange is having a technology issue, dozens of members may be reaching out to that exchange's market operations staff, sales representatives and other contact points with requests for information and status, perhaps multiple times. During an incident, there could be literally hundreds of communications via telephone or e-mail as basic and innocuous as "we are having an issue" or "we may be having an issue" or "we

don't know the root cause." Over the next several weeks, in the normal course of interactions with members, exchange representatives may get asked dozens of times effectively "what happened?"

Direct Edge respectfully submits that efforts to re-create and analyze these myriad interactions would add little value and create unintended consequences. For example, SCI Entities may need to develop policies instructing employees to avoid any and all communications with members and other market participants regarding SCI Events, save what is publicly disseminated via Rule 1000(b)(5). Senior executives and media relations personnel may shy away from discussing prior events with the media, or from providing disclosures regarding what is not the root cause of an event (like a cyber-attack). Accordingly, Direct Edge does not believe that Proposed Rule 1000(b)(4)(iv)(C) advances the overall objective of improved disclosure of SCI Events to the marketplace and should thus be eliminated.

- Direct Edge respectfully suggests that the requirement of "immediate" notification is unrealistic and could trigger an innumerable amount of "false alarms". Given the broad definition of what an SCI Event would be, many of them will be discovered only after a fair amount of investigation regarding exception reports and other information generated by an SCI Entities IT compliance and governance infrastructure. If SCI Entities are required to notify immediately, that will effectively become a requirement to notify when there is a mere suspicion of the existence of an event, leading to less overall utility regarding said notifications. SCI Entities should only be required to notify the Commission "upon confirming the existence of an SCI Event".

e. Proposed Rule 1000(b)(5) – Member Notification

Subject to its comments above regarding the scope of the definition regarding "Dissemination SCI Events", Direct Edge supports Proposed Rule 1000(b)(5) as written.

f. Proposed Rules 1000(b)(6) and 1000(b)(8) – Notification of Material System Changes

Direct Edge believes Proposed Rule 1000(b)(6) should be eliminated in its entirety, and Proposed Rule 1000(b)(8) be utilized as the primary vehicle for Commission notification of material changes an SCI Entity's systems. Proposed Rule 1000(b)(6) is built on the faulty premise that the Commission should bear responsibility for a minutely-detailed understanding of the IT infrastructure of all SCI Entities and be in a position to assess prospective changes thereto – and the potential impact on resiliency, redundancy, integrity and security – in advance of their implementation. This concept runs contrary to the basic underpinning of Reg SCI – that the SCI Entity itself is responsible for its own systems and their compliance with Reg SCI and other applicable regulations and obligations. While the Commission needs, and deserves, an understanding of how an SCI Entity's infrastructure changes over time, it is not realistic to expect the Commission to be a bulwark against changes that may have unintended or deleterious consequences.

Subject to a modified definition of "material system change" as discussed above, Direct Edge strongly suggests reliance on Proposed Rule 1000(b)(8)'s requirement of periodic reporting regarding such changes as a more effective complement to the event-based communications required under Proposed Rule 1000(b)(4). Such reporting would provide an important supplemental tool for the Commission in its oversight and understanding of how SCI Entities are complying with their responsibilities, without imposing unrealistic expectations to review and prevent incidents before they occur.

g. Proposed Rule 1000(b)(7) – Review of Systems

Direct Edge supports Proposed Rule 1000(b)(7) as written. The rule should be clarified, however, to state that any review of a Processor under an NMS Plan be performed independently of reviews of the same entity in other capacities (*e.g.*, as an exchange or other SCI Entity).

h. Proposed Rule 1000(b)(9) – BCP & DR Testing

Direct Edge comments on Proposed Rule 1000(b)(9) are subject to its comments on Proposed Rule 1000(b)(1) regarding the fundamental distinction between BCP and DR. So long as these disciplines are conflated in the rule, its enforcement will be problematic. For example, testing by an SCI Entity of its BCP capabilities – which certainly should occur – cannot be coordinated with members as Proposed Rule 1000(b)(9)(i) would require. The entire point of such BCP testing would be to not coordinate it with customers, and assess whether operations out of BCP facilities was seamless to members and other market participants.

Commenting on the proposed rule primarily from a DR perspective, Direct Edge is concerned about the scope of the proposal in two primary respects:

- Mandating "rapid recovery" creates potential risks that SCI Entities must choose between putting the safety of their employees and market participants at risk, and a Reg SCI violation. At a minimum, Reg SCI should state that even where DR capabilities exist and are ready for use, other factors may exist that would justify the delay of operations from DR facilities. With the one-year anniversary of Superstorm Sandy upon us, Direct Edge respectfully suggests that a regulation that even implies a demand to "trade no matter what" is not appropriate.

- The requirement to coordinate DR testing is unlikely to meaningfully reduce risk unless it is narrowed significantly in scope. Coordination without a targeted set of objectives will only marginally increase industry readiness and provide little incremental information about the overall readiness of critical market infrastructure. Direct Edge recommends the coordinated testing requirements be limited to the providers of singular services in the market, namely:

    - Exchanges that list securities;
    - Exclusive processors under NMS plans; and
    - Clearing and settlement agencies

  If market participants' own systems and DR plans are compatible with the plans of this limited sub-set of SCI Entities, there would be greater system-wide confidence in the market's operational resiliency.

IV. Conclusion

Direct Edge would like to thank the Commission again for providing us with the opportunity to offer our comments on Reg SCI. The Commission and its staff should be commended with a forward-looking approach in this area, which is all too easy to ignore until the inevitable system-wide event occurs. We look forward to being a productive contributor to the dialogue regarding Reg SCI in any forum the Commission and its staff deem advisable and desirable.

Sincerely,

William O'Brien
Chief Executive Officer

cc: Hon. Mary Jo White, Chair
Hon. Luis A. Aguilar, Commissioner
Hon. Daniel M. Gallagher, Commissioner
Hon. Kara M. Stein, Commissioner
Hon. Michael S. Piwowar, Commissioner

John Ramsey, Acting Director, Division of Trading & Markets
James R. Burns, Deputy Director, Division of Trading & Markets
David S. Shillman, Associate Director, Division of Trading & Markets
Heather Seidel, Associate Director, Division of Trading & Markets
Gregg Berman, Associate Director, Division of Trading & Markets
David Hsu, Assistant Director, Division of Trading & Markets