July 10, 2013

Elizabeth M. Murphy
Secretary
Securities and Exchange Commission
100 F. Street N.E.
Washington, D.C. 20549-1090

RE: Regulation Systems Compliance and Integrity; Exchange Act Release No. 69077; File No. S7-01-13

Dear Ms. Murphy:

BATS Global Markets, Inc. ("BATS" or "the Exchange") appreciates the opportunity to comment on the above-referenced Securities and Exchange Commission ("SEC" or "Commission") rule proposal ("Regulation SCI" or the "Proposal"), which is intended to ensure that the U.S. securities trading markets develop and maintain systems with adequate capacity, integrity, resiliency, availability, and security, and reinforce existing requirements that such systems operate in compliance with the Exchange Act. In general, Regulation SCI would require so-called SCI entities, including registered national securities exchanges, registered national securities associations, clearing houses, and some ATSs, to establish written policies and procedures reasonably designed to ensure that their systems have levels of capacity, integrity, resiliency, availability, and security adequate to maintain their operational capability and promote the maintenance of fair and orderly markets and that they operate in the manner intended. It would also require SCI entities to mandate participation by designated members or participants in scheduled business continuity and disaster recovery plans.

In addition, Regulation SCI would require notices and reports to be provided to the Commission regarding, among other things, SCI events and material systems changes. SCI events would be defined under the Proposal to include, with no *de minimus* thresholds, systems disruptions, systems compliance issues, and systems intrusions. Under the Proposal, an SCI entity would be required to immediately report an SCI event to the Commission when any responsible SCI personnel becomes "aware" of it, and the Proposal would require most SCI events to be reported to members or participants of the SCI entity. With respect to material systems changes, Regulation SCI would require, absent exigent circumstances, SCI entities to provide the Commission with 30-days advance notice of any such changes, and subsequently provide the Commission with updates if a previously disclosed material systems change becomes materially inaccurate. The Proposal also would require SCI entities to conduct an annual review of their compliance with Regulation SCI, and submit that report, as well as management's response to the report, to the Commission within specified timeframes.

At the outset, BATS would like to note concern about the potential overlap between Proposed Regulation SCI and the Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*.[1] This Directive is aimed at strengthening the security and resilience of the United States' critical infrastructure against physical and cyber threats.[2] Critical infrastructure is defined in this Directive as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[3] National securities exchanges likely fit within this definition as well as the definition of "SCI entities" in Regulation SCI, potentially bringing the Directive and Regulation SCI into conflict and increasing the burden imposed on SCI entities. BATS requests that the Commission explicitly account for this potential overlap in determining whether to adopt the requirements outlined in the Proposal.

I. Background

Proposed Regulation SCI comes at a time when entities covered by the Proposal are already highly incented to avoid the occurrence of an SCI event because of competition with one another, as well as an industry-wide desire to avoid high impact events such as the flash crash in 2010. While BATS generally supports the goal of adopting regulations under the Exchange Act to match the highly interconnected, increasingly automated, modern securities markets, BATS believes that to preserve innovation and competition, any such regulation needs to be flexible and allow room for evolution.

In today's market, the national securities exchanges compete vigorously against one another and against broker-dealer execution platforms and cannot afford to develop a reputation for technology problems. Consequently, the exchanges spend millions of dollars each year maintaining and upgrading their technology, as well as recruiting and retaining the best available technology and operations professionals. The effect of this competition can be seen directly from the rate of change year over year in self-help declarations. Each self-help declaration reflects a technology problem in which a national securities exchange's protected quotation is inaccessible in an automated fashion, as explained in Regulations NMS.[4] When an exchange has

---

1 Office of the Press Secretary, Exec. Office of the President, Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil; *see also* Exec. Order No. 13636, 78 Fed. Reg. 11739 (2013). The Department of the Treasury is the sector-specific agency responsible for the financial services industry under the Presidential Directive. Office of the Press Secretary, *supra*.

2 Office of the Press Secretary, *supra* note 1.

3 *Id.*

4 *See* Regulation NMS, 70 Fed. Reg. 37496, 37519, 37521–22, 37535 (June 9, 2005), *available at* http://www.sec.gov/rules/final/34-51808.pdf (self-help declarations are discussed in the context of Rule 611).

self-help declared against it, the market seamlessly routes around that exchange until the problem is resolved, a fact that alone demonstrates the resilience of our equities market today. The instances of an exchange experiencing a technology problem requiring self-help has dramatically decreased. In 2011, BATS Z-Exchange declared self-help against another exchange 33 times, while in 2012, that number decreased to eight, and for 2013 year-to-date, that number stands at five.[5] BATS believes this data reflects technology enhancements by exchanges that are a direct result of the competitive environment in which exchanges operate.

Additionally, while fragmentation can heighten the potential for systems problems originating from any number of sources that broadly affect the market, the industry has responded with several targeted initiatives in recent years to address this concern. In particular, in the wake of the flash crash in 2010, the exchanges implemented single stock circuit breakers, followed recently by the implementation of limit-up, limit-down across the equity markets. These measures are designed to prevent trading beyond predefined dynamic limits, thereby avoiding problems associated with a temporary liquidity void or a runaway algorithm that could otherwise have a cascading effect through the market. In addition, the exchanges have either implemented or will be implementing risk management controls on an exchange-by-exchange basis that can be used as a "kill switch" to automatically stop a member or participant's trading when certain pre-defined risk management thresholds are triggered. BATS deployed these risk management controls on its equity and options exchanges in November 2012, and anticipates that this functionality will be centralized at the Deposit Trust and Clearing Corporation (DTCC) in the near future, thereby providing real time, inter-market risk management to the industry. All of these factors should be considered by the Commission in determining the extent to which each of the requirements of proposed Regulation SCI should be adopted.

Given the highly interconnected and technological nature of the modern securities markets, BATS believes Regulation SCI must be flexible enough to preserve innovation and competition. The Commission appears to recognize this need and has attempted to address it by framing the Proposed Regulation as a "reasonable policies and procedures" rule. Nonetheless, BATS believes that, absent further refinement and definition, many requirements of the current proposal would require an operational and compliance infrastructure that would be overly burdensome and impractical to implement. In particular, with respect to the reporting obligations proposed in Regulation SCI, because of the lack of clear definition surrounding some of those obligations, covered entities will be compelled to monitor and report numerous routine events to the SEC on a daily basis to avoid an enforcement action in the case of the inevitable technology disruption.

In addition, while the Commission ostensibly has left to the industry the task of defining the policies and procedures that would be reasonable to implement to achieve the goals of the Proposed Regulation, the Commission has also proposed, as examples, policies and procedures that in some cases, particularly with respect to software development, are far more burdensome than those commonly deployed in the financial services industry. As a result, BATS is again concerned that in the inevitable instance of an SCI event, a covered entity's failure to implement

[5] *See* BATS EXCHANGE, *Alerts*, http://batstrading.com/alerts.

the precise policies and procedures suggested by the Commission will form the basis for an assertion in the context of an enforcement action that the covered entity's policies and procedures were not reasonable. We do not believe this is the Commission's intent; however, we are concerned that this is the manner in which Regulation SCI may be enforced.

II. SCI Systems and SCI Security Systems

A. SCI Systems

Proposed Regulation SCI defines SCI systems to mean "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, or order routing, market data, regulation, or surveillance."[6] According to the Proposal, the definition is intended to "reach those systems traditionally considered to be core to the functioning of the U.S. securities markets."[7] BATS has several concerns regarding the scope of this definition. First, BATS is concerned about the regulatory arbitrage associated with including order routing systems within the definition of SCI systems. While national securities exchanges support order routing, they do so in competition with smart order routers offered by a wide-variety of broker-dealers that are not covered by the rule. BATS believes the inclusion of order routing as an SCI system, with all the attendant obligations thereby imposed on those systems under Proposed Regulation SCI, puts it at a competitive disadvantage vis-à-vis those other broker-dealer offerings. Moreover, BATS finds the inclusion of order routing in the definition of SCI systems to be curious in light of one of the key policy rationales underpinning the Proposal—the enhancement of investor confidence—when, in fact, the vast majority of orders from retail investors are routed and executed away from the national securities exchanges by broker-dealers that would not be subject to Regulation SCI.

Second, BATS is concerned about the inclusion of those systems operated by third parties on behalf of an SCI entity that would otherwise meet the definition of an SCI system if they were operated directly by the SCI entity.[8] The inclusion of vendor-provided systems within the definition of SCI systems raises several concerns associated with an SCI entity's ability to ensure compliance with the Proposal's requirement that the vendor adopt reasonable policies and procedures, as well as requirements related to reporting SCI events to the SEC and/or the SCI entity's members or participants. BATS believes it will be difficult, if not impossible, for SCI entities to ensure that their third party vendors comply with the requirements of Regulation SCI because, to ensure such compliance, these vendors would be required to disclose to SCI entities highly detailed information about their intellectual property and proprietary systems.

---

6 Regulation Systems Compliance and Integrity, 78 Fed. Reg. 18084, 18099, 18177–78 (proposed March 25, 2013) (referring to Proposed Rule 1000(a)).

7 *Id.* at 18099.

8 *See id.*

Consequently, many necessary relationships between SCI entities and third party vendors may be foreclosed, forcing SCI entities to insource functions more efficiently performed by vendors. The cost of this insourcing will be passed along to members and market participants and may degrade competition. BATS questions the extent to which the Commission has analyzed the costs and benefits of this aspect of the proposal.

Third, BATS questions the need to include regulatory and surveillance systems within the definition of SCI systems.[9] Unlike those systems that are core to trading, a problem with a regulatory system—which could be an automated surveillance or an automated case management system—poses no immediate threat to trading or the market in general. By its nature, even when surveillance is conducted in real time, very little can be done with that real-time information. The investigative process is often lengthy, involving efforts to identify patterns of misconduct in some cases, an iterative dialogue with members, and intensive periods of analyses by investigators and attorneys. If a surveillance or other regulatory system experiences a problem, it can easily be corrected and restored, and, if necessary, historical data can be run or rerun through the surveillance system. Such problems do not impact the functioning of the market associated with them. Accordingly, BATS requests that the Commission reconsider the inclusion of regulatory and surveillance systems within the definition of SCI systems.

B. SCI Security Systems

Proposed Regulation SCI defines the term "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."[10] BATS is again concerned about the scope of this definition. As proposed, BATS believes it is difficult to define the endpoints of the systems covered by the rule. In particular, the lack of clarity associated with the manner in which systems must share network resources to constitute SCI security systems is problematic. BATS believes those systems that are physically segregated from SCI systems would not be considered SCI systems under the Proposed Rule. Yet, in many cases, segregation takes the form not of physical barriers, but of logical barriers. In the latter case, logical barriers can be circumvented; however, SCI entities such as BATS go to great lengths to prevent and monitor for such circumventions. It is not clear from the Proposed Rule whether the Commission intends for these logically segregated systems to be included within the definition of SCI security systems. BATS is concerned that if the Commission does intend for these systems to be included, then an employee's personal computer could be considered an SCI system to the extent that the employee has the capability to access an SCI entity's network remotely through, for example, a virtual private network, or VPN. In such a case, it is not clear how an SCI entity could ensure that its employees' personal computers could comply with the requirements of the Proposed Rule associated with the adoption of reasonable policies and procedures and the reporting of SCI events.[11] BATS

---

9 *See id.*

10 *Id.* at 18099, 18177 (referring to Proposed Rule 1000(a)).

11 *See* 78 Fed. Reg. at 18178–79 (referring to Proposed Rule 1000(b)(1), (4)–(5)).

suggests excluding from the definition of "SCI security systems" those systems where there is a logical segregation from SCI systems, so long as the SCI entity monitors the system for security breaches and has the ability to shut the system off if it detects a security breach.

III. Reasonable Policies and Procedures

A. Industry Standards

Proposed Regulation SCI requires covered entities to establish, maintain, and enforce written policies and procedures designed to ensure that its SCI systems and 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.[12] To this end, proposed Regulation SCI includes several required areas of coverage—capacity planning, capacity stress testing, systems development, testing, business continuity and disaster recovery plans. According to the Proposal, the policies and procedures that are adopted to comply with Regulation SCI are "reasonably designed if they are consistent with current SCI industry standards."[13] The Commission did not seek to define precisely what those current industry standards are; however, the Commission did propose, by way of example, several freely-available publications that it believes reflects industry standards that would be in compliance with proposed Regulation SCI.[14]

While the Commission is ostensibly leaving some discretion to SCI entities in determining what current industry standards to adopt, the mere fact that the Commission has articulated a list of publications that it believes reflect current industry standards creates some concern that a failure to rigidly adopt those publications will subject a covered entity to an accusation that the standards it did adopt were not current industry standards in the inevitable occurrence of an SCI event. In this regard, BATS is concerned that the actual standards proposed by the Commission are not, in fact, always reflective of common industry practice. For example, the Commission has proposed National Institute of Standards and Technology (NIST) standards regarding the software development lifecycle.[15] These standards reflect an approach to software development that contains burdensome, staged processes and that contemplate teams working independently on a software project in *seriatim* at each stage of the process.[16] This approach, also known as the waterfall methodology, is generally considered inefficient and obsolete. While such standards may be deployed today in some large government contract

---

12 *Id.* at 18091–92, 18107, 18178 (referring to Proposed Rule 1000(b)(1)).

13 *See id.* at 18107, 18178–79 (discussing the requirements of Proposed Rule 1000(b)).

14 *Id.* at 18109 (referring to the publications contained in Table A).

15 *Id.* at 18111.

16 *See generally* NIST Security Considerations in the System Development Life Cycle (Special Publication 800–64 Rev. 2), *available at* http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf.

projects, we do not believe they are in use in the financial services industry, which generally adheres to more nimble processes based in part on what is known as Agile Software Development. Under this more nimble approach, software development is integrated in such a fashion as to encourage and facilitate iterative collaboration across business, regulatory, and compliance units throughout each stage of development, leading to small, controlled, regular rollouts of upgraded software. Utilizing the more proscriptive processes contemplated by the NIST standards would likely lead to fewer, and consequently larger, rollouts of upgraded software, which we believe increases the risk of a technology failure.

B. Testing After Implementation

The Proposal requires SCI entities to "establish, maintain, and enforce written policies and procedures" that are "reasonably designed to provide for . . . [p]eriodic testing of all [SCI] systems and any changes to such systems *after their implementation*."[17] This requirement is in addition to a separate provision in the Proposal requiring SCI entities to "establish, maintain, and enforce written policies reasonably designed . . . to provide for ongoing monitoring of the functionality of [SCI] systems to detect whether they are operating in the manner intended."[18] Given the existence of these two separate requirements, we believe the Commission intends with respect to the former to require SCI entities to conduct regression testing after code has been implemented and released into the production environment. While BATS and other SCI entities conduct extensive regression testing of code in the pre-production environment (before the code is implemented), BATS believes it unnecessary and unreasonable to conduct the same type of testing after implementation. There is no basis to believe that re-running such tests would uncover any issues that were not discovered in the pre-production environment, and, hence, we do not believe the proposed requirement will help ensure the capacity, integrity, resiliency, availability, and security of SCI systems. Instead, BATS believes that it should be sufficient to monitor SCI systems for compliance with the federal securities laws and all relevant rules and regulations. Therefore, BATS requests that the Commission consider deletion of the proposed requirement to periodically test such systems after their implementation.

IV. Reporting Requirements for Certain SCI Events

The Proposal requires an SCI entity to immediately report to the Commission upon any responsible SCI personnel becoming aware of a systems disruption that the SCI entity reasonably estimates would have a material impact on its operations or on market participants, any systems compliance issue, or any systems intrusion.[19] The Proposal further requires an SCI entity to submit a more detailed report of such events to the Commission within 24 hours, and submit subsequent reports as Commission staff may reasonably request until the SCI event is resolved.[20]

---

17 78 Fed. Reg. at 18115, 18178 (emphasis added) (referring to Proposed Rule 1000(b)(2)(ii)(2)).

18 *Id.* at 18115, 18178 (referring to Proposed Rule 1000(b)(2)(ii)(4)).

19 *Id.* at 18118, 18178 (referring to Proposed Rule 1000(b)(4)(i)).

20 *Id.* at 18118, 18178–79 (referring to Proposed Rule 1000(b)(4)(ii)–(iii).

The Proposal further requires these SCI events to be promptly reported by an SCI entity to its members and participants; although, the Proposal permits an SCI entity to delay the reporting of information about systems intrusions to members and participants when the SCI entity affirmatively determines that such reporting would compromise the security of its SCI systems or SCI security systems, or an investigation of the systems intrusion.[21] Finally, the Proposal requires SCI entities, absent exigent circumstances, to provide 30-days advance notice to the Commission of any planned material systems changes.[22] BATS has several concerns about the scope and timeframes of these various reporting requirements.

A. Responsible SCI personnel

BATS is concerned about the scope of employees that could be considered to be responsible SCI personnel. As defined, responsible SCI personnel means "any personnel, whether an employee or an agent, of the SCI entity having responsibility for" an SCI system or SCI security system.[23] We believe it will be difficult for SCI entities to determine the full scope of individuals that fall within the definition of responsible SCI personnel. The guidance from the Commission in the Proposal is not particularly illuminating, other than to clarify that individuals who have no responsibility for an SCI system are not responsible SCI personnel.[24] Additional guidance in the Proposal makes clear that the Commission intends for the scope to be broad and cover both senior and junior level employees if they have any responsibility vis-à-vis an SCI system or SCI security system.[25] The lack of clarity with respect to what the Commission means by "responsibility" for an SCI system or SCI security system, combined with the Commission's clear intent that the scope be broad, covering both senior and junior level employees, is concerning because the reporting requirements in the rule are triggered by responsible SCI personnel becoming aware of an SCI event.[26]

Similarly, BATS is concerned about the "becomes aware" standard underlying these reporting requirements. In BATS' experience, it is often not immediately clear when BATS and its personnel have in fact become aware of SCI events. For example, in the case of systems compliance issues, a junior employee may identify a particular occurrence or a customer may report some perceived problem to the Trade Desk, and it may then take several hours or days of research and analysis before BATS can determine whether the event in question was actually a systems compliance issue. In such cases, when did responsible SCI personnel become aware of

---

21 *Id.* at 18119, 18179 (referring to Proposed Rule 1000(b)(5)).

22 78 Fed. Reg. at 18122, 18179 (referring to Proposed Rule 1000(a)).

23 *Id.* at 18117–18, 18177.

24 *Id.* at 18118.

25 *Id.*

26 *See id.* at 18178–79 (referring to Proposed Rule 1000(b)(4)–(5)).

the SCI event? The answer to this question is important because, again, under the Proposal, awareness triggers mandatory reporting requirements.

BATS is also concerned that in the inevitable instance of an SCI event, the Commission may, as a matter of course, second guess the timing of an SCI entity's reporting of SCI events based on its own investigation of which particular employees are "responsible SCI personnel" and when they became "aware" of the SCI event. We believe that these standards will have the unintended effect of impeding competition and innovation by making it difficult for SCI entities to attract and retain employees who might be considered SCI personnel under the proposal. Such employees may be legitimately concerned about personal liability associated with their employment. BATS believes a more prudent approach would be to trigger the mandatory reporting obligations upon senior officers becoming aware of accurate and actionable information. Given, as BATS noted at the outset, the shared interests the industry has with the Commission in avoiding SCI events, BATS believes this standard is a more balanced and rational approach to achieving the goals of the Proposal.

B. Systems Disruptions

Pursuant to the Proposal, reportable SCI events include systems disruptions. Systems disruptions in turn are defined to include: "(1) [a] failure to maintain service level agreements or constraints; (2) [a] disruption of normal operations, including a switchover to back up equipment with near-term recovery of primary hardware unlikely; (3) [a] loss of use of any SCI system; (4) [a] loss of transaction or clearance and settlement data; (5) [s]ignificant 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 systems components or queuing of messages to or from customers of such duration that normal service delivery is affected."[27] BATS believes the proposed definition of a systems disruption is impracticably broad and will include minor and routine systems issues that do not materially affect an SCI entity's performance of core functions.

For example, BATS does not understand the Commission's interest in an SCI entity's failure to maintain service level agreements, which reflect privately negotiated contracts and may have no material impact on the delivery of core services to customer(s). In fact, in some cases, a private contract may have more stringent requirements than required by regulation, which would have the perverse effect under the Proposal of transforming service level agreements into new regulatory obligations.

Similarly, BATS does not understand the Commission's interest in a switchover to back-up equipment if that switchover has no material impact on the delivery of core services to customers. BATS has built-in redundancy throughout its systems, and seamless failovers to redundant equipment is part of normal operations. For example, BATS systems failover to redundant power supplies several times per month without causing any disruption in service

[27] 78 Fed. Reg. at 18178 (referring to Proposed Rule 1000(a)).

delivery. Under the Proposed Regulation, SCI entities would have to report every such instance of power failover. SCI entities would also have to report to the SEC every time a disk in a Redundant Array of Independent Disks (RAID group) failed or degraded such that the performance of that hard drive minimally deteriorates. BATS expects this type of failover to occur within its systems at least three to four times per month and, industry-wide, these hard drives have built-in redundancy to make such failures fairly unnoticeable to market participants. In a similar vein, BATS receives redundant data feeds from other markets to enable the Exchange to quickly failover to a non-preferred feed when the preferred feed is slow or problematic, which is another fairly frequent and unnoticeable event that SCI entities would have to report. Moreover, BATS conducts nightly maintenance on its systems requiring a failover to different connections. It is not clear from the Proposal's language whether such regularly-scheduled maintenance outside of trading hours would also be included under the umbrella of "disruption of normal operations." BATS does not believe it would be practicable or reasonable to require near-real time reporting of non-impactful events such as these. At a minimum, BATS believes an adequate and balanced approach would require an SCI entity to include such information in an annual report to the Commission, rather than in near real-time reports to the Commission.

BATS finds more alarming the Commission's inclusion of "a queuing of data between system components or queuing of messages to or from customers of such duration that normal service delivery is affected"[28] in the definition of systems disruption. According to the Proposal, the Commission is of the view that the "queuing of data between systems components of SCI systems is often a warning signal of significant disruption of normal system operations."[29] In fact, however, the queuing of data between systems components is a normal and necessary occurrence as information moves between systems components. Any time messages are sent from system component to system component, messages may be buffered (i.e. queued) in several places. Data queuing at the application level or some lower level is likewise normal, necessary, and non-problematic. In fact, data queuing caused by congestion control within common network protocols is fundamental and essential in handling the variable bandwidths and flow of messages that are central to the market today. For example, the Transmission Control Protocol/Internet Protocol (TCP/IP), which is a standard set of internet protocols used for data transmission, is designed to slow down any time it appears that the data recipient is having trouble receiving the data. This kind of data queuing occurs multiple times to multiple market participants every week without causing any kind of material disruption in the markets. Furthermore, data queuing can also occur at much lower levels within a network where reporting is often difficult, and sometimes impossible, depending on the infrastructure of the hardware vendor and the visibility its devices offer to customers. In as much as queuing of data occurs on an ongoing basis throughout the day, it would not be reasonable to expect that an SCI entity should or could report to the Commission every instance in which such queuing is occurring, nor is it clear what the Commission would do with such information. We believe that the queuing of

[28] *Id.* at 18178 (referring to Proposed Rule 1000(a)).

[29] *Id.* at 18102.

data should only be a reportable event to the extent that it materially affects the delivery of core services to customers.

Similarly, BATS takes issue with that aspect of the proposal in which the Commission states its preliminary belief that customer complaints or inquiries about a slowdown or disruption of operations, such as a slowdown or disruption in their receipt of market data is indicative of an SCI entity experiencing a systems disruption.[30] In BATS' experience, customer reports regarding delays are often caused by some external problem and are unrelated to the operation of BATS' internal systems.

Moreover, the Commission notes in the Proposal that a disruption of normal operations is intended to "capture problems with SCI systems such as programming errors [and] testing errors."[31] To the extent this can be read to include programming errors and testing errors that occur prior to production, BATS does not understand the policy rationale to support such a requirement. Obviously, during the pre-production testing phase for any new code, programming errors, as well as errors in the tests developed for such code, are discovered and corrected. These are routine occurrences throughout the software development process and are the reason for that process in the first instance. To the extent the Commission intends to require reporting of such occurrences, BATS questions the policy rationale underlying such requirement. The burden associated with such reporting would be significant, and we question its value in the context of the Proposal's goals. To the extent the Commission does not intend for such instances to be reported, we respectfully request that the Commission clarify the requirement.

Finally, BATS questions the extent to which the Commission has adequately considered the costs associated with the Proposal's reporting requirements. According to the Proposal, the Commission anticipates 65 reportable SCI events per year per SCI entity under Regulation SCI.[32] The Commission did not attempt to further breakdown the anticipated reportable events into the reporting subcategories—systems disruptions, systems intrusions, and systems compliance issues. However, BATS believes the Proposal could require each SCI entity to report hundreds of systems disruption events each year alone; although, the vast majority of such events would be virtually unnoticed by market participants. In order to comply with the Regulation, BATS believes it would need to hire several new employees simply to fulfill the reporting obligations. BATS asks that the Commission reconsider, based on comment letters it receives, the adequacy of its cost analysis under the Proposal.

C. Systems Intrusions

30 *Id.*

31 *Id.* at 18101.

32 78 Fed. Reg. at 18148.

The Proposal defines a "systems intrusion" as "any unauthorized entry into the SCI systems or SCI security systems of an SCI entity."[33] Any time responsible SCI personnel become aware of a systems intrusion, the SCI entity must immediately notify the Commission.[34] The Commission makes clear in the Proposal that this requirement will apply to both intentional and unintentional conduct leading to such unauthorized entry.[35] Thus, if an employee accidentally clicked on a link containing a computer virus, the SCI entity would be required to notify the Commission within 24 hours, even if the mistake had no impact on SCI systems. BATS is concerned that such a broad requirement would unreasonably and unnecessarily burden SCI entities and the Commission because SCI entities will have to rapidly investigate and report a multitude of minor incidents that regularly occur during the normal course of business. BATS believes the cost of complying with such a rule outweighs any benefit that would accrue as a result of collecting such information. Instead, BATS suggests that policies and procedures reasonably designed to prevent, detect, and respond to such systems intrusions should be sufficient to achieve the desired outcome of this proposed rule.

D. Immediate Reporting of SCI Events to the Commission and Prompt Reporting to Members and Participants

As previously noted, the Proposal requires an SCI entity to "immediately" report "a systems disruption that the SCI entity reasonably estimates will have a material impact on its operations or on market participants, any systems compliance issue, or any systems intrusion."[36] The Commission expects immediate reporting to occur regardless of the time of day any responsible SCI personnel becomes aware of the SCI event.[37] This immediate report, which can be done orally or via email, is then required to be followed by a written notification within 24 hours, followed by regular written updates until the SCI event is resolved.[38]

BATS is concerned with the rigid reporting requirements required by the Proposal. In particular, a requirement to immediately report, day or night, the existence of an SCI event when any responsible SCI personnel becomes aware of it raises significant compliance concerns. As explained above, and particularly related to the existence of a systems compliance issue, it has been BATS' experience that it can take a day or more of research and analysis to fully determine whether a systems compliance issue exists. In such cases, BATS again is concerned that its employees will be second-guessed regarding the precise moment "awareness" occurs. BATS appreciates the Commission's need to be apprised of SCI events, but BATS questions why this

---

33 *Id.* at 18103, 18178 (referring to Proposed Rule 1000(a)).

34 *Id.*at 18118, 18178 (referring to Proposed Rule 1000(b)(4)(i)).

35 *Id.* at 18103.

36 *Id.* at 18118, 18178 (referring Proposed Rule 1000(b)(4)(i)).

37 *See* 78 Fed. Reg. at 18118–19.

38 *Id.* at 18118, 18178–79 (referring to Proposed Rule 1000(b)(ii)–(iii)).

need cannot be met by a requirement that SCI events be reported promptly to the Commission with follow-up reporting required, not within "24 hours," but at such frequency as is thereafter reasonably requested by Commission staff.

In addition to requiring disclosure to the Commission, proposed Regulation SCI would require SCI entities to disclose detailed information about "dissemination SCI events" to all members or participants.[39] The Commission proposes to define a "dissemination SCI event" as "an SCI event that is a: (1) Systems compliance issue; (2) Systems intrusion; or (3) Systems disruption that results, or the SCI entity reasonably estimates would result, in significant harm or loss to market participants."[40] The Commission acknowledges in its commentary that "public disclosure of each and every systems issue . . . could be counterproductive," and as a result, the Commission has limited the disclosure of systems disruptions to those disruptions that could result in significant harm or loss to market participants.[41] The Commission has not, however, similarly limited the scope of reporting for systems compliance issues. This is concerning because often times an immaterial systems disruption can also be considered a systems compliance issue—the two definitions are not mutually exclusive. Consequently, while an immaterial systems disruption is not required to be reported to members and participants, if the event is also considered a systems compliance issue, it would be. In BATS' experience, this can in fact be counterproductive. In particular, in some cases, a systems compliance issue may impact few members or participants, may be of brief duration, and/or may involve little to no member/participant harm. In such cases, BATS does not believe it would be productive to require broad dissemination to all members and participants.

With respect to both requirements regarding reporting to the Commission as well as reporting to members and participants, BATS suggests that the Commission consider implementing a *de minimus* threshold below which SCI entities would not be required to make such reports. At a minimum, BATS suggests that with respect to *de minimus* SCI events, the Commission limit the number of members and participants SCI entities are required to inform to those members and participants that are, or are reasonably expected to be, affected by the *de minimus* SCI event. Whether an SCI event is *de minimus* could depend on: (1) the number of participants affected by the event; (2) the dollar value of the potential harm from the event; (3) the duration of the event; and (4) the amount of time the event is expected to continue to persist.

E. Material Systems Changes

The Proposal requires SCI entities to notify the Commission of all "material systems changes" at least 30 days before such changes would be implemented, absent exigent circumstances.[42] While the proposal provides some examples of what the Commission considers

---

39 *Id.*at 18178 (referring to Proposed Rule 1000(b)(5)).

40 *Id.* at 18104, 18177 (referring to Proposed Rule 1000(a)).

41 *Id.* at 18104.

42 78 Fed. Reg. at 18122, 18178 (referring to Proposed Rule 1000(b)(6)).

to be "material" systems changes, those examples, which all derive from prior Automation Review Policy ("ARP") interpretative guidance, suggest the Commission intends to require SCI entities to report far more systems changes than BATS would consider to actually be "material" and, frankly, far more than what is currently reported to ARP by entities covered by the ARP program.[43] In particular, the Commission gives the following description of things it preliminarily believes are material:

> major systems architecture changes; reconfigurations of systems that would cause a variance greater than five percent in throughput or storage; the introduction of new business functions or services; changes to external interfaces; changes that could increase susceptibility to major outages; changes that could increase risks to data security; changes that were, or would be, reported to or referred to the entity's board of directors, a body performing a function similar to the board of directors, or senior management; and changes that could require allocation or use of significant resources.[44]

BATS is concerned about the breadth of routine matters that could meet these standards and with the vagueness inherent in such phrases as "the introduction of new businesses or services," "changes that *could* increase susceptibility to major outages," "changes that *could* increase risks to data security," and "changes that *could* require allocation or use of significant resources."[45] Like other SCI entities, BATS is continually updating and improving its system architecture to make its systems better and more efficient, and there are dozens of changes each week that BATS might consider reportable under the standards articulated in the Proposal. BATS is concerned about the compliance burden and attendant impact on competition and innovation associated with the requirement to file these reports, and questions the value and productive use of this information to Commission staff. BATS further questions the adequacy of the Commission's analysis of the costs associated with the requirement to file reports of material systems changes. As noted in the Proposal, the Commission staff believes that each SCI entity would report approximately 60 material systems changes *per year*.[46] However, based on the description of the Commission's view of materiality, BATS believes it could be reporting that many material systems changes *per week*. Therefore, BATS asks that the Commission reconsider the adequacy of its cost analysis under the Proposal.

At present, BATS reports material systems changes to ARP based on those changes that are reported to BATS' Board of Directors, which we believe captures the full scope of material changes about which the Commission ought to be concerned. Moreover, ARP has never indicated any dissatisfaction with this level of reporting. As such, BATS requests that the

---

43 *See id.* at 18105–06.

44 *Id.*

45 *Id.*at 18105–06 (emphasis added).

46 *Id.* at 18151.

definition of materiality be modified to include only those systems changes that are reported by an SCI entity to its board of directors or body performing a function similar to a board of directors.

BATS is also concerned about the 30-day advance notification of material systems changes requirement. As proposed, the only exception to this 30-day standard is based on exigent circumstances, examples of which include systems compliance issues or systems intrusions requiring immediate corrective action.[47] In the absence of exigent circumstances, it would be a violation of Regulation SCI to implement a material systems change without providing notice and then waiting 30 days.[48] While such a construct could be sensible if the Commission's definition of materiality was significantly narrowed, given the breadth of the Commission's proposed interpretation of materiality, as discussed above, this 30-day notice requirement will significantly burden SCI entities and degrade competition and innovation.

V. SEC Access to SCI Systems and SCI Security Systems

Pursuant to the Proposal, SCI entities would be required to grant SEC staff access to their SCI systems and SCI security systems.[49] The Commission stated its belief in the Proposal that such a requirement is consistent with the existing inspection requirements contained in Section 17 of the Securities Exchange Act ("the Exchange Act").[50] BATS questions this conclusion. Under Section 17, Commission staff is accorded the right to inspect certain books and records of covered entities.[51] Such a requirement is fundamentally different from that contained in the Proposal, which would expand the Section 17 requirement to one that would provide Commission staff access to SCI entities' production and live security systems.[52] BATS does not believe such access is currently contemplated by Section 17 of the Exchange Act, and BATS has significant concerns about being required to provide unbridled access to such systems in an uncontrolled fashion to any third party, governmental or otherwise. BATS respectfully requests that the Commission reconsider both its authority for this requirement under the Exchange Act, as well as the practical concerns it raises for SCI entities.

* * * * *

BATS appreciates the opportunity to comment on Proposed Regulation SCI. Please feel free to contact me at (918) 815-7000 if you have any questions related this matter.

---

47 78 Fed. Reg. at 18122.

48 *See id.*

49 *Id.* at 18130, 18180 (referring to Proposed Rule 1000(f)).

50 *Id.* at 18130, 18180.

51 15 U.S.C. § 78q(b).

52 *See* 78 Fed. Reg. at 18130, 18177–78, 18180.

Sincerely,

Eric J. Swanson
Secretary

cc: The Honorable Mary Jo White, Chairman
The Honorable Elisse B. Walter, Commissioner
The Honorable Luis A. Aguilar, Commissioner
The Honorable Troy A. Paredes, Commissioner
The Honorable Daniel J. Gallagher, Commissioner

John Ramsey, Acting Director, Division of Trading and Markets
James R. Burns, Deputy Director, Division of Trading and Markets
Dave S. Shillman, Associate Director, Division of Trading and Markets
David Liu, Senior Special Counsel, Division of Trading and Markets