



105 WESSON TERRACE, NORTHBOROUGH, MA. 01532

TEL: 212 809 3800

[www.tellefsen.com](http://www.tellefsen.com)

April 19, 2013

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

**Re: SEC Proposed Rule – Regulation SCI SEC File No. S7-01-13; Release No. 34-69077**

Dear Ms. Murphy:

We are pleased to provide you with our comments and views about the SEC's proposed rulemaking on Regulation SCI (Systems Compliance and Integrity).

The enclosed perspectives are our own and do not necessarily reflect the views of major exchanges, investment banks, broker dealers, automated trading systems, trading platform providers or industry organizations.

**Background:**

Tellefsen and Company, L.L.C. ("TCL") is a boutique management consulting firm founded by Gerald Tellefsen in 1984. Since then, the firm has been exclusively focused in the global capital markets, derivatives and financial services industries.

Over the years, we have worked for numerous market constituents - major U.S. equity, options and futures exchanges, clearing organizations, futures commission merchants, securities broker-dealers, investment banks, proprietary trading and asset management firms.

Two of our major, relevant practice areas include market structure/micro structure consulting and business continuity management ("BCM"), which we believe qualifies us to provide domain expertise, industry insight and direct working knowledge guidance to the Commission.

In our market structure practice area, we have consulted to equity, exchanges, ECNs, ATs, interdealer brokers, start-up markets and other market participants on the workings of the equity, options and futures markets.

In the market micro structure arena, we have assisted these entities with the development of comprehensive system testing strategies and plans. These have included user acceptance testing, quality assurance testing, stress and failover testing, etc. Most of these assignments have been relative to SEC ARP or CFTC Core Principles compliance.

In the business continuity management practice area, we have consulted to exchanges, clearing houses, investment banks, broker dealers, futures commission merchants, investment management firms and proprietary trading firms. We have developed BCM strategies for these entities, as well as comprehensive business continuity and disaster recovery plans.

We have also conducted independent attestation oversight and reporting for market participants that are so required, as part of their regulatory compliance.

We have consulted and provided our counsel to these market participants on their business continuity strategies and plans, technology and network architectures and set ups for key, mission critical systems (i.e., electronic trading, order management, market data dissemination, price reporting, clearance and settlement, surveillance and risk management).

Our firm has been actively involved with the Futures Industry Association ("FIA") for over 15 years and our principals have been members of the FIA Information Technology Division.

In this capacity, John Rapa has chaired the FIA's Business Continuity Committee and coordinated the annual industry DR testing since 2003.

### **Proposed Reg SCI Rulemaking:**

The Commission has developed a proposed rulemaking that, if enacted, would require "SCI entities" (self-regulatory organizations, operators of automated trading systems, electronic communications networks, market data plan processors, exempt clearing agencies) - and potentially securities based swap execution facilities and swap data repositories – to be compliant.

The main thrust of Reg SCI encompasses enhanced approaches and sound practices to the development, management, operation and maintenance of mission-critical systems that support fair and orderly markets.

Reg SCI is intended to require SCI entities to implement, manage and oversee more rigorous processes, procedures, systems and compliance controls to protect against system disruptions, unauthorized network security intrusions and the potential for systemic risk.

At present, the Commission seeks to establish mandatory standards for the operation of mission-critical trading and market data dissemination functions by SCI entities, SCI SROs and plan processors.

These entities are those organizations which would be deemed "critical" financial markets or systemically important order flow and liquidity providers by the Commission – in the event that a wide-scale, significant business disruption ("SBD") impacts their operations.

The proposed regulation would enhance and replace the Commission's current Automation review Policy ("ARP"), and also impact certain aspects of Reg ATS.

In this regard, the Commission seeks, among other things, to have the designated SCI SROs establish a same-day recovery time objective ("RTO") and to maintain a to-be-defined geographic dispersal of their infrastructure and personnel, so that they can achieve the same-day RTO in the event of a *wide-scale SBD*.

The Commission seeks input and counsel as to what should be within the scope of Reg SCI and what should not.

The Commission also seeks to require SCI entities to conduct adequate, regular testing and review of their automated trading and clearing systems to ensure proper system functioning, adequate capacity and security.

Business Continuity Management is analogous to Operational Risk Management. From our perspectives, most of these organizations do an excellent job in this area and have been diligent in their BC/DR planning and implementations for many years.

From our direct experience and working knowledge of the major exchanges and clearing houses, they have built out and evolved their technology infrastructures and networks in the last 3-5 years and have designed resiliency, redundancy and fail over capabilities into their mission critical system architectures.

They have learned valuable lessons from the September 11, 2001 disasters, the Northeast blackout of 2003, Hurricanes Rita and Katrina and most recently Hurricane Sandy. They have become sensitive to the potentials for physical threats, terrorist attacks, acts of God/nature, cyber terrorism, software worms, spoofing, pandemics etc.

The exchanges, ATSS, member firms and clearing houses have refined their strategies, plans and tactics accordingly via regular testing and enhancements to processes and procedures. The backdrop of this has been commensurate with:

- The growth of electronic trading / reduction in open outcry trading
- Market fragmentation of equities and options
- Introduction of new products, new systems, new business lines
- Globalization of trading and clearing constituents
- Growth and introduction of proximity hosting, algorithmic trading, high frequency trading, direct market access
- The availability of new system and network technologies and tools that are faster, cheaper and better than their previous generations
- New technologies and tools that can identify/isolate network and/or system faults, facilitate system failover/roll back capabilities
- Modern tools and technologies that allow them to remotely manage data centers, systems, servers and networks, failover/roll back systems, load balance systems and networks – with limited technical staffs
- Regulatory evolution
- Technologies that have redundant hardware components and/or software tools to facilitate backup and recovery capabilities.

#### **Comments and Areas of Concern:**

We have reviewed the proposed rulemaking as it would apply to SCI entities and have comments, observations and concerns in the following areas:

1. Scope and Applicability
2. Business Continuity Resilience
3. Testing
4. Information Security
5. Estimated Scope and Costs of Testing
6. Market Evolution and Preparing for the Unknown

## **1. Scope and Applicability:**

The scope and applicability of the proposed Reg SCI should address the unintended consequences of the fragmentation of the equity and options market created by Reg NMS in 2005.

In this regard, those organized exchanges, ATS and ECNs, market data plan processors, which are deemed “systemically important” to the fair and orderly operations of the US capital markets should be subject to its compliance.

In addition, as the remaining aspects of Dodd-Frank crystalize, securities based swap execution facilities (“SEFs”) and possibly swap data repositories (“SDRs”) should also be required to be compliant.

The proposed rulemaking goes into great detail to suggest what the quantitative trigger points should be that would require an entity to become compliant, and thus be designated an “SCI entity”.

Much of the language appears to be borrowed from the existing Reg ATS volume and market share trigger points for dark pool/ATs (e.g., >5% market share in any NMS eligible name in 4 of the 6 preceding months or >.25% in all NMS eligible names).

However few, if any, ATs today have breached this. Of the approximately 30 reporting and non-reporting dark pool/ATs tracked by the Tabb Group today, only four have a “matched market share” of 10% or greater, with most of the others having no more than a 4%-8% share (Source: *Tabb Group Liquidity Matrix*, March 2013).

It does not appear that these ATs have breached the Reg ATS market share trigger points. In anticipation of breaching any of these regulatory levels, they have the ability to turn off or “delist” an issue.

In our opinion, the existing Reg ATS threshold trigger points are adequate. Given the state of market fragmentation, these should be re-visited, depending on feedback and comments to the proposed rulemaking.

Taking the demographics of order flow providers, the proliferation of algorithmic trading, high frequency trading and flow trading into consideration, even the smallest, least capitalized, tech savvy traders can rapidly flood the market with thousands of orders, cancellations and messages that have the potential to slow down, clog or disrupt even the best tested and most resilient exchange or ATs trading infrastructure.

## 2. Business Continuity Resilience:

Given the above background, it remains to be seen as to the depth and extent of the human capital pool and skill sets that exist in SROs and ATs in both their primary and backup site locations.

In today's economic times, it is not practical to have all key job functions fully duplicated, geographically dispersed and housed in both locations (e.g., operations, compliance, finance, risk management, etc.), nor is it economically feasible for these organizations to hire, train and retain such redundant staffs.

There also has been much publicity and opinions about the need for exchanges, ATs and other trading platform providers to have "kill switches" that can be triggered if there are disruptions similar to the Flash Crash, Knight, BATS or NASDAQ problems.

The concept of a kill switch is a great idea, but in reality no exchange or trading platform provider will ever implement a system that abdicates the control of the market or system's operations to a totally automated kill switch function.

If more trained eyeballs were looking at control screens during the above problems, humans would have intervened and common sense would have/should have prevailed. Fast moving, fragmented markets need smart technologies as well as smart humans overseeing them.

We would counsel the Commission to get more objective feedback from senior technologists who have built and implemented large complex trading systems, as well as senior management from exchanges that are responsible for trading operations. These individuals should have experience with the vagaries and nuances of trading, as well as how to best handle disruptions "on the fly", while maintaining fair and orderly markets.

We believe that the Commission's proposed rulemaking also stops short in a few areas, namely:

- While the proposed rulemaking seeks enhanced BCM standards for SCI entities there is no mention of a same day RTO for their major constituents (e.g., liquidity providers, futures commission merchants, global clearing firms, plan processors, data vendors, etc.). What is the expectation for these market constituents?
- If the Commission expects that if an SCI SRO or ATs will achieve a same day RTO, will their "significant" liquidity providers and clearing firms also be required to have this capability ? (Note: a general 80-20 rule of thumb might be that 20% of firms typically supply 80% of the order flow, liquidity or clearing capability on a daily basis).
- What is the expectation of an SCI SRO or ATs if a SBD occurs during the latter part of the business day (e.g., 2:00 PM)? Would they be expected to recover that same day?

- Given the amount of transactions that may have been done, failover and recovery of executed transaction files could conceivably take longer than if it occurred earlier in the day, thus cascading past the close of the market.
- Should there be a rule as to what portion of a trading day constitutes a full day (e.g., analogous to the seventh inning rule for a complete ballgame).
- Once an SCI entity is deemed “critical” by the Commission, how quickly will they be required to comply with the new standards, implement, test and demonstrate same?

### 3. Testing:

The proposed rulemaking calls for a more rigorous and mandatory approach to testing by SCI entities, with the goal of testing mission-critical systems and operations under “more realistic” market conditions.

The proposed regulation seeks to require SCI entities to conduct periodic system testing and to be sufficiently resilient and geographically dispersed to be able to ensure a next day resumption of trading and a 2 hour resumption of clearance and settlement services.

It also mandates participation by “designated members or participants” in scheduled testing of BC/DR plans with SCI entities.

From our direct knowledge of the major equity and options exchanges and numerous ATS, they already perform a number of testing initiatives as part of their resiliency and obligations to operate fair and orderly markets:

- As exchanges, ATSS, trading platform providers and clearing houses have introduced new systems, applications, products and system functions, their internal IT staffs have conducted regular system testing, regression testing, stress testing, failover testing etc., to ensure their availability, capacity, resilience and readiness
- These organizations regularly augment IT testing with other BCM exercises (e.g., they conduct annual BC/DR plan updates, building evacuation drills, business disruption scenario planning workshops, etc.)
- In addition, all the U.S. exchanges and clearing houses have participated in the planning and execution of the annual DR test initiative conducted and coordinated by the FIA and Securities and Financial Markets Association (SIFMA).
- These industry tests were started after the events of September 11th 2001 and are now entering their 10<sup>th</sup> year.
- The FIA and SIFMA industry-wide tests have involved a tremendous amount of planning, foresight and coordination.

As the Chair of the FIA's Business Continuity Committee, I can attest that thousands of man-hours of preparation are required to prepare for and execute the annual industry test (see Section 5, Estimated Scope and Costs for Testing, below).

When the FIA Business Continuity Committee was started in 2002, one of the original goals was to establish a weekend date where most/all firms can test with the various exchanges they belong to once annually, as opposed to testing with multiple exchanges on multiple dates throughout the year.

The industry test has been intended to provide the opportunity for exchanges and their members and major service providers to test their backup systems and sites and leverage the economy of scale of doing it all on one day. It has not yet been intended to be a scenario exercise (e.g., neighborhood or key service provider outage, Lower Manhattan outage, Chicago Loop outage).

Since most of these firms are constantly making changes to their infrastructures and environments, there are a lot of "moving parts" and the potential for many things to go wrong.

The firms and exchanges have found the annual industry testing valuable - to be able to test the resilience of their infrastructure, and fail over to their backup systems and facilities, to ensure they work "as designed" and "as specified".

Unless they have an actual disruption, invoke DR and fail over during the course of the year, they do not have the opportunity to ensure that their networks, firewalls, systems and infrastructure really work as expected.

The FIA and SIFMA industry tests have not been mandatory, but both industry groups have enhanced the scope of testing, encouraged and engaged more firms, exchanges and market entities to participate each year.

Both industry groups have developed and enhanced the process to engage the exchanges, clearing houses and firms, educate them on the scope of the testing and manage the overall test process.

This has been honed over time to easily "on board" new member firms, participants and exchanges.

In 2012, for example, the annual FIA industry test involved 18 exchanges and clearing houses, 68 futures commission merchants and 46 trading participant firms. The exchanges reported that the firms that tested represented ~80% of their clearing members and that these firms do ~85% of their 2012 volumes.

See the enclosed link to the 2012 industry test results on the Futures Industry Association website: <http://www.futuresindustry.org/business-continuitydisaster-recovery.asp>

The exchanges typically engage their mission critical production and backup systems and facilities for the test. As part of the scope, it is expected that firms typically fail over from production to their backup systems/sites.

Since no changes to application software code are anticipated, the backup should function identically to production. Typically, firms are required to enter a “small but meaningful” amount of orders in specified products, from which the exchanges will send execution reports.

This is intended to test the efficacy of round trip communications of orders, quotes, execution reports and related messages. The intent is that if firms can enter a few orders in DR mode effectively, they can trade.

However, given the scope of these tests, they are not designed to be “stress tests”, given the complexities of orchestrating a stress test with so many players across multiple markets on a Saturday.

We suggest that the Commission consider that at any given time, there will never be a 100% participation of all market participants in testing, no matter how much advanced planning is done (e.g., we have had firms cancel on the day before the industry tests due to changes in internal operational schedules and priorities).

SCI entities should be allowed to consider an “80-20” approach to mandatory testing, i.e., typically 20% of the firms might provide 80% of the order flow or liquidity.

If SCI SRO and ATS entities can engage their key order flow and liquidity providers that collectively provide at least 80% of their total transaction volumes, they should have a core nucleus of liquidity, and thus be capable of managing a fair and orderly market.

If SROs and ATSs require their “systemically important” order flow and liquidity providers to test and encourage as many of the rest to do the same, one can conclude that they should be prepared and can manage a fair and orderly market with that subset.

With all this said, the best system testing strategies, written procedures and policies, robust capacity planning and state of the art technologies are *not designed for multiple events all going wrong at the same time.*

Embarking on an industry test that involves multiple constituents that is scripted to create the response and reaction to multiple, adverse and concurrent events will involve significant advanced planning, input and discussion as to the scope and objectives.

To carve out a scope for such an undertaking will take many months of advance planning with dozens of constituents. At this point, we believe that it is speculative to suggest that this type of scenario exercise is even feasible to achieve.

#### 4. Information Security:

Information security breaches, website hacking and denial of service attacks are constant and growing threats in today's wired world, and global financial services firms have been the target of many of these disruptions or attempts.

The proposed regulation calls for increased vigilance and hardening of information security ("InfoSec") controls for their mission critical systems and information.

We believe that as part of the proposed regulations, SCI entities should be required to demonstrate the scope and extent of their InfoSec controls, technology infrastructure, processes and written procedures.

This should include, but not be limited to activities such as regular, independent reviews of network security, controls, network penetration tests and policies and procedures to identify, isolate and mitigate the effects of InfoSec breaches.

Independent, network intrusion detection tests should be conducted, *both from outside an SCI entity's firewalls and from within*. Testing should be conducted by qualified, independent network security firms in concert with the SCI entity.

Testing should encompass, but not be limited to: network intrusion, penetration testing, phishing attempts, worms, virus, denial of service attacks, etc.

InfoSec systems, processes and procedures should encompass the SCI entities' mission critical systems (e.g., order management, risk management, trade matching, clearance/settlement), as well as any web portals, internal shared drives and systems that support the management and administration of their business (e.g., finance, operations, administration, regulation, surveillance etc.)

However, we feel strongly that, as proposed in Rule 1000(f), that SCI entities should *never* allow the Commission to have online access to its systems, either remotely or on site.

While the SCI entity should be required to demonstrate their controls, technology safeguards and procedures, it is imprudent to allow a third party (the Commission) to have this level of access.

Furthermore, given the nature and rate of change with network technologies and related infrastructure, we believe it is *not realistic* for the Commission to expect to have the quantities and qualities of expertise required to attempt this, let alone to be able to stay current with these technologies.

## 5. Estimated Scope and Costs for Testing:

The Commission has provided dozens pages of estimates of the manpower required for SCI entities to be compliant with the proposed regulation. This is part of the Paperwork Reduction Act.

But we feel there are aspects that this tome has underestimated. We would like to add to what has been drafted, based on our 10 years of experience in planning, managing and overseeing industry test initiatives, and working with numerous exchanges, clearing houses and market participants.

There are dozens of man-days of pre-test planning, preparation, pre-test testing, testing and post-mortem reviews associated with the industry test initiatives. There are anywhere from tens to hundreds of business and technology staff members engaged in this initiative. These include, but are not limited to:

- Operations managers
- Operations specialists
- Network engineers
- Network managers
- IT managers
- Information security engineers
- Business continuity managers
- Key service providers

In our professional estimates, we believe that, on average, the staffing levels required to support these types of test initiatives are as follows:

<u>SCI Entity:</u>	<u>Estimated #Man Days:</u>
• Exchanges	175-200+
• Member Firms	80-85
• ATS	12-25

In addition to large scale industry tests, all of these entities conduct regular and ad hoc testing of mission critical systems for the introduction of new software releases, new features and functions, system upgrades etc.

The staffing required to plan and conduct those tests is generally 10% -20% of the above estimates on average.

## **6. Market Evolution and Preparing For The Unknown:**

We hope that the Commission receives thoughtful and insightful feedback and suggestions from market participants as to how the proposed Reg SCI should be implemented.

Given the current state of market fragmentation in U.S. equities and options markets, and the near term view that this will probably continue before any consolidation occurs, we urge the Commission to consider market evolution and unknowns as it solidifies its approach to the proposed regulations.

Market impacting events such as the 2010 Flash Crash, the botched BATS IPO, the Knight Capital algo that “went rogue” and the crush of orders and cancellations associated with the euphoria of the Facebook IPO cannot be easily foreseen nor adequately tested for.

The next major headline event will not necessarily be the same as these. The biggest unknown is the impact from the law of unintended consequences.

Much of the issues that the Commission seeks to resolve have been caused by the volume and velocity of trading created by market fragmentation (e.g., algo trading, smart order routing, inter-market sweep orders, co-location etc.).

As our markets evolve, our regulation and compliance oversight needs to evolve in lock step. In order to do this, we need smart regulation to be able to evolve hand in hand with smart technologies.

## Conclusions, Going Forward:

In our professional opinion, most/all of the SCI entities have the technology and network infrastructure and procedures in place to address the spirit of what the Commission is seeking.

However, the general rule of thumb in BCM is that *one size does not fit all*. The Commission should implement a workable approach, commensurate with the size and scale of the respective SCI SROs, ATSS, and consider how each of them are set up and organized to achieve them.

We suggest the Commission look to the exchanges, ATS and key trading platform providers for their feedback about the quantity and quality of their labor pool and how they are staffed and organized with the capacity to recover from a SBD.

If rushed to implement, a broad based approach to these new standards may only be as good as the weakest link that exists – the slowest, least capitalized organization that is the last one to have this capability in place.

Regular and varied testing will be key to corroborating industry readiness going forward.

*In today's fragmented, sub-millisecond high-speed markets, we need smart regulation, not more regulatory crush...*

Our best counsel to the Commission is to analyze the feedback from the comment period, and assess the time frames that the major exchanges, ATS and key trading platform providers indicate that they can adopt the new standards.

We would be pleased to continue the dialogue with you and other industry constituents. We will be available for any follow up questions or to discuss the state of industry sound practices in this area.

Very truly yours,

*John J. Rapa*

John J. Rapa, CBCP  
President/Chief Executive Officer

TELLEFSEN AND COMPANY, L.L.C.