



David Lauer  
Market Structure and Technology Architecture Consultant



July 8, 2013

VIA ELECTRONIC MAIL

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

Re: Proposed Regulation Systems Compliance and Integrity  
Securities and Exchange Commission (“SEC” or “Commission”)  
Release No. 34-6907; File Number S7-01-13 (March 7, 2013)

Dear Ms. Murphy:

I appreciate the opportunity to provide comments to the proposed Regulation Systems Compliance and Integrity (“Regulation SCI” or the “Reg SCI”), issued by the Commission in Release No. 34-6907; File No. S7-01-13, dated March 7, 2013.

### **Bio**

I am a Market Structure and Technology Architecture Consultant. I am one of very few, independent voices in the market structure debate. I represent no industry organization or company, and am simply trying to help share my years of expertise in the hope that what results can help improve capital markets, and the US economy. I have testified before the Senate Banking Committee and appeared on the SEC Technology Roundtable in the wake of the Knight Capital incident that was the beginning of the Regulation SCI development process. I have been working on electronic trading platforms, both developing them and using them, for the past 8 years. My previous work includes technology architecture at IEX Group, electronic trading at Allston Trading and Citadel Investment Group, and as an early employee at Tervela.

### **Introduction**

“I believe that our conceptual apparatus for understanding drift into failure is not yet well-developed. In fact, most of our understanding is held hostage by a Newtonian–Cartesian vision of how the world works. This makes particular (and often entirely taken-for-granted) assumptions about decomposability and the relationship between cause and effect. These assumptions may be appropriate for understanding simpler systems, but are becoming increasingly inadequate for examining how formal-bureaucratically organized risk management, in a tightly interconnected complex world, contributes to the incubation of

failure.” - Sidney Dekker, [Drift Into Failure](#)

Regulation SCI is one of the most important regulations that the SEC has formulated since Regulation NMS. The equity markets have evolved and changed dramatically since Regulation NMS was approved and implemented. The most critical change has been to technology systems. While these systems have obviously been critical and central to the functioning of markets and firms for decades, it is not until more recently that we've witnessed such extreme proliferation and reliance on them for the functioning of our markets and provision of liquidity.

The advent of High Frequency Trading, Algorithmic Execution Services, and the dramatic fragmentation of our markets has combined to create an unfathomably complex system. The importance of this cannot be overstated, and must be understood and agreed upon by everyone before delving deeper into the specifics of Regulation SCI. The rapid advance and adoption of advanced technology has transformed a complex, non-linear system, resulting in a very different, complex, non-linear system. Regulators and market participants had many decades of experience with the previous system, but the current one is relatively new to us.

Regulation SCI is an attempt to control a complex system. This is an inherently Sisyphean task. While that does not mean it is an unworthy goal, and it is certainly worth pursuing, it must be recognized from the very beginning that it is nearly impossible. This attitude must be embraced, rather than dismissed. Technology systems fail. There is no amount of testing, certification or standards that will prevent this from happening. The worst mistake that regulators can make with this effort is to assume that:

1. They can prevent technology failures.
2. Previous failures are prescriptive of future failures, and therefore provide a roadmap to prevent them.
3. That “glitches” or “bugs” are simple failures of process or controls. That there is a direct cause-and-effect relationship, where if the cause is addressed, the effect can be changed or prevented.

These are the tenets of systems theory and complex systems. Sidney Dekker's book [Drift Into Failure](#) should be required reading for anybody who seeks to regulate a complex system, and certainly for anyone charged with writing rules around complex technology systems. The orientation and philosophy that he espouses is essential if there is to be any hope of dealing with the evolution of our technology and financial systems.

“System thinking is about relationships, not parts. System thinking is about the complexity of the whole, not the simplicity of carved-out bits. Systems thinking is about non-linearity and dynamics, not about linear cause-effect-cause sequences. Systems thinking is about accidents that are more than the sum of the broken parts. It is about understanding how accidents can happen when no parts are broken, or no parts are seen as broken.” - Sidney Dekker, [Drift Into Failure](#)

If there is to be any doubt, this is exactly the attitude that Dr. Nancy Leveson was discussing on the SEC Technology Roundtable, on which I was honored to participate. In her opening statement, she said:

“The third and final practice I want to talk about is the application of systems thinking and system engineering. These industries realize the problem is not just a technology problem; that they need to design the larger system so that software errors don't cause mayhem because they know that the software errors are going to occur despite what they do.”

...

“The financial industry needs to learn, too, that computers aren't magic; that our engineering techniques

for creating software aren't perfect; and that failsafe and fault tolerant designs, whether these features are automated or they use humans in a monitoring function, are a goal but not yet a reality.”

These points are critical to understand and internalize. Despite our best efforts, failure will not be averted. In many cases, our attempts to prevent technology failures, such as kill switches, will only make things worse. Our primary goal should be to design the right incentives for participants, and when those incentives fail, ensure that broad, strong technology standards are mandated for nearly all direct market participants. Doing so will ensure that when failure does occur, the market will react appropriately and resiliently, and will give us the best chance to “weather the storm” and recover as gracefully as possible. We cannot have the goal to prevent failure, “bugs,” “glitches,” or “incidents.” They will happen. The focus should instead be on reducing their frequency and containing their impact, to the greatest extent possible. In addition, transparency should be the core of every approach to technology and broader market reforms, so that the greatest number of participants can learn from others' mistakes and successes.

## **Responses to Questions**

The Regulation SCI proposal is clearly a substantial one, and it would be difficult to address all of the questions that it contains. I will therefore choose several questions from throughout the proposal to address what I believe are the most important issues that should be resolved before the final rule is drafted. I believe this to be the most reasonable and readable approach. I hope that my comments are substantive and helpful, and would be happy to follow-up in-person, on the phone or by email. I will also only focus on questions pertaining to equity markets, as that is my area of expertise.

### **Question 1: Definition of SCI Entity**

This very first question is perhaps one of the most politically charged questions in the document. The Commission has defined SCI Entities as ““SCI self-regulatory organization, SCI alternative trading system, plan processor, or exempt clearing agency subject to ARP.” I would urge the Commission to broaden the definition to include any entity with direct electronic access to equity markets, especially to that of broker-dealers, about which Question 192 seeks comment. This is, most certainly, not a popular viewpoint (and this sentence is the most dramatic understatement in my entire Comment Letter). I believe, however, that the definition of SCI Entity is a holdover of ARP, upon which SCI is based. The scope of ARP (i.e. the entities it applied to) was sufficient in a different market context, when the market was human-centered and generally slower. The market has changed, and I urge the Commission to adapt to this change more aggressively and dramatically.

In its current state, the US equity market can be disrupted by a single server sending hundreds of thousands of orders per second via a hardware-accelerated system over extremely high-speed network connections. While the Market Access Rule is designed to ensure robust technology standards, it does not come close to the SCI proposal. We need more specificity in mandated standards, and Regulation SCI is an excellent start. It will prove to be far more effective if the scope is broadened to include any firm that has direct electronic market access, and therefore to supercede that part of the Market Access Rule. We cannot leave the health of our marketplace in the hands and judgment of participants, this has proven to be a disastrous approach thus far.

In the summary to his Comment Letter, Dr. James Angel states that: “Market participants have the right economic incentives to protect themselves from catastrophic events, but not necessarily to protect the market as a whole.” I strongly disagree that market participants have the proper incentives to protect themselves. This laissez-faire attitude should have been discredited by now, either by the 2007 financial crisis, or the innumerable technology incidents (most notably Knight Capital) that we've witnessed over

the past few years. Every firm in every industry is constantly balancing the cost of safety with scarcity of resources. The Commission's job in this regard is to compel these firms to act in their own long-term interests, and the interests of the public at-large, rather than any short-term interests that may be better served by underinvestment and cutting corners.

Again, I realize that this response would make the SCI proposal far more difficult to pass. That being said, just because something is difficult, does not mean it should not be pursued. The industry will lobby aggressively against such a plan, which should be an indication that it is probably a good idea. I hope the Commission considers this proposal, because it would transform the industry's technology standards and address current technology problems in a far more holistic and systems-wide context.

### **Question 3: Significant-Volume ATS**

Along the same lines as my response to Question 1, I will make a similarly unpopular statement in response to the definition of an ATS and specifically a “significant volume” ATS. I will start by quoting the rule proposal itself. The purpose of the change in definition of “significant volume ATS” is stated: “to ensure that proposed Regulation SCI is applied to an ATS that could have a significant impact on the NMS stock market as a whole, as well as an ATS that could have a significant impact on a single NMS stock and some impact on the NMS stock market as a whole at the same time.”

However, further along in the rule proposal, “The Commission notes that its analysis of the OATS data does not reveal an obvious threshold level above which a particular subset of ATSs may be considered to have a significant impact on individual NMS stocks or the overall market, as compared to another subset of ATSs.”

I believe that based on this quote, every ATS should be defined as an SCI Entity, and should have to comply with Regulation SCI. Any ATS can impact the market, and any participant on any ATS can have a disproportionate impact on the market. It makes no sense to have arbitrary and subjective thresholds or limits where there is no compelling reason. Our current framework leans far too much on encouraging competition in the marketplace, to the detriment of the market itself.

Fostering competition is undoubtedly an important and admirable goal. This does not mean that it should be elevated above ensuring a stable and technologically robust marketplace. We must consider several things that I have emphasized repeatedly. The current market is a complex system. The nature of a complex system is sensitive dependence on initial conditions, and is susceptible to the butterfly effect. This means that every participant and every venue can have an outsized and dangerous impact on the marketplace. I therefore urge the Commission to consider the danger of excluding any ATS, and therefore providing a gateway not just for technology problems and failures, but of security risks as well.

### **Questions 4, 5, 6 and 7: Significant Volume Thresholds**

I would once again urge the Commission to eliminate any subjective or arbitrary thresholds when delineating which entities are subject to Regulation SCI. If that is not possible, I would urge the Commission to choose thresholds that account for at least 99% of all entities. This would ensure that the entire market is protected, while still providing a space for new entrants to get started.

### **Question 13: Threshold Measurement Period**

If the Commission keeps thresholds in the final rule, measurement periods should be made far more aggressive. New SCI Entities will not be subject to the requirements of Regulation SCI for 6 months based on this proposal. There is no reason for such a buffer period, and it is dangerous. Those entities not subject to Regulation SCI that suddenly find themselves transacting a substantial amount of equity

market volume in NMS stocks are likely to be the least tested, the most prone to failure, and represent one of the most dangerous holes in this proposal. With our ability to quickly measure and react to changing market dynamics, this period should be shortened to be at most “two of the preceding four weeks” rather than “four of the preceding six months”.

### **Question 19: SCI System and Security System Definition**

As stated earlier, I believe SCI systems should include any technology system that has direct market access. I would additionally extend that statement to the SCI Security System as well. Any server that is able to place orders into our market is a tremendous security risk. This should be seen from the perspective of a regulator as well as from that of national security. Security tends to be an after-thought generally, and I applaud the Commission for making it a focal point of Regulation SCI, and for the broad definition that has been chosen. I agree that any system that may provide a jumping-off point into other systems that can directly impact the market must be made part of Regulation SCI and should have robust and strictly mandated security standards. It is difficult to define these systems in a limited way – often the worst security failures are a result of systems that nobody realized were linked or accessible. Therefore, the Commission should mandate independent security audits, and that independent auditor should have latitude to define which systems are included and which can be safely excluded.

### **Questions 23 and 24: SCI Security System Inclusion**

It is critical that the Commission include Security Systems in Regulation SCI. The interconnected nature of technology systems means that failure is generally difficult to isolate or even predict. While much of what we have seen in financial services has been confined to mistakes or programming bugs, that does not mean that hacking attacks should be disregarded. This is admirably proactive of the Commission, and critically important. Technology systems are only as strong and stable as the weakest element, and must be considered in the context of every technology system and vulnerability within the infrastructure.

In addition, I urge the Commission to examine broad, independent security standards such as those established by the OSSTMM (Open Source Security Testing Methodology Manual)<sup>1</sup>, and consider it for inclusion. The OSSTMM has been recommended by the NIST, the Treasury Dept. Office of Thrift Supervision, and is supported by many other governmental and non-governmental entities, including NASA, the Whitehouse, the Vatican, and many major international financial institutions. It is the most robust and open standard on the market, and can provide critical guidance on properly securing SCI systems.

### **Question 29: Definition of System Disruption**

This definition seems reasonable and broad enough. This must be caveated by understanding that the seventh proposed element, “a queuing of data between system components or queuing of messages to or from customers of such duration that normal service delivery is affected,” while being a very good indicator of a problem, is not necessarily being properly monitored by most firms. Therefore, compliance with Regulation SCI should involve clearly demonstrating that queue depth is being effectively monitored throughout the infrastructure, rather than just at the point where messages are transmitted to/from customers. This should include all input/output pathways, and at every level of the infrastructure stack, including:

1. Network-level
2. Middleware-level
3. Application-level

---

1 <http://osstmm.org>

The Commission must be very specific with regards to monitoring queue depth, as it is easy to interpret the proposed rule as only pertaining to network-level queues on switches and routers. These are often not where problems materialize or are revealed. It is rather on the application- and middleware-level that the first indication of a problem becomes evident. This is another area in which pushback should be expected, as it will incur cost to properly and effectively monitor these systems. That being said, there is no substitute for monitoring systems to this extent, and any technologist will tell you that it is critical to getting early warning for potential problems / failures.

### **Question 33: Inclusion of Quantitative Thresholds**

The Commission is taking on a difficult task in trying to delineate specific time periods, for example. Setting a 100 millisecond threshold could result in this part of the regulation becoming completely outdated within the span of a year or two. Instead, I think it makes far more sense for SCI Entities to benchmark and baseline their systems in a robust manner, under realistic high-volume conditions. Establishing a proper baseline performance is a critical first step, and one all entities should undertake. At that point, the Commission can establish relative thresholds, i.e. a one or two standard deviation move from baseline, in order to be considered a disruption. These baselines must be demonstrable to be robustly derived, and the Commission should err on the side of overreporting, rather than underreporting. In addition, baselines should be reestablished annually, or any time a major infrastructure change is made.

### **Question 34: Other Types of Disruptions**

The Commission asks “ if an SCI SRO or SCI ATS suspects a technology error originating from a third party (such as an SCI SRO’s member firm or an SCI ATS’s subscriber) that has the potential to disrupt the market, should that type of discovery be included in the definition of systems disruption?” This question would not pertain if my previous guidance to extend the reach of Regulation SCI is heeded and all direct access participants are included. If that is not done, then this should absolutely be included in the definition of a systems disruption. Once again it is critical that any incidents that impact the broader market, regardless of their source, are identified and contained. In addition, if any forewarning is possible that there may be a technology problem occurring or about to occur, information must be quickly and accurately disseminated.

### **Question 63: Interval for Capacity Tests**

The Commission should specify a relative period for capacity tests, which could be defined as anytime required system capacity increases by 10%, for example. This is far more robust than trying to mandate a time period. If a time period mandate is required, it should be quarterly at a minimum. In addition, anytime there is a material systems change as defined previously in the Regulation, capacity planning must be part of the rollout of such a change.

### **Question 66: Testing**

While the areas to be tested are comprehensive, it is critical that the Commission mandates that such testing must be done by independent groups in addition to regular testing done by the groups that have designed or built these systems. While I was the lone voice on the Technology Roundtable arguing this point, it is important to have independent testing performed – such testing cannot be done properly and robustly by those involved in the design and/or development of such systems. This is not to disregard the importance of testing by those people, it is merely to stress the importance of diversity. This is another point towards the development and maintenance of complex systems. When analyzing and testing such systems, diversity of perspectives is critical to prevent group-think and narrow testing within design goals/guidelines. Independent testing and quality assurance groups are standard in many other industries, and should be so within Financial Services as well.

**Question 71: Kill Switches**

Static Kill Switches are a horrible idea, plain and simple. The effect would most likely be to exacerbate an already unstable situation by depriving the market of order flow and liquidity at times of stress. Once again, I stress the importance of understanding the nature of our current market and the high level of complexity. The kill switches as proposed by the Industry Working Group are quite simply a disaster waiting to happen. In addition, they will be ineffective even when operating properly because they are confined to individual exchanges and market centers.

Proper kill switches can only be implemented as part of the market-wide surveillance system I have proposed many times. Kill switches must be built intelligently, with the perspective of every market center. These dynamic, adaptive kill switches should be able to properly baseline systems, even to the extent of being done on a per-algorithm basis, and within the context of the broader market. Such systems would be able to identify when a system is behaving erratically rather than when the entire market is undergoing a stressful event. I urge the Commission to prevent any type of static kill switch from being rolled out, and instead address this problem properly.

**Question 80: Barriers to Entry**

It should seem clear that mandating these standards will increase the barrier to entry to SCI Entities. However, that should be a design goal of Regulation SCI rather than something to be feared. This regulation should not be restricted because of such a fear. I sincerely hope that the Commission uses this opportunity to reduce the complexity of our current market, rather than relaxing standards in order to add ever more complexity.

**Question 82: Publications in Table A**

I once again encourage the Commission to include the OSSTMM (Open Source Testing Methodology Manual) in both Information and Physical Security. It provides robust, specific methods for securing and testing complex infrastructure, in addition to providing a holistic, systems-wide approach to security, rather than security in isolation. ISECOM, the non-profit group that publishes this manual is widely recognized throughout the security industry as being one of the foremost authorities on security, and their fundamentally open approach is perfectly in-line with the Commission requirements for inclusion in Table A.

**Question 88: Cost Burden**

As I have stated many times, cost burden should not be an appropriate reason to omit an SCI entity. If the burden to ensure secure, stable systems is too much, that entity should not be allowed to be in a position to impact the market.

**Questions on Safe Harbor**

The Safe Harbor provision is a dangerous one. It creates the same misalignment of incentives that Regulation SRO does in limiting liability. The threat of enforcement and liability is a far better motivator than the notion that as long as one has produced all proper documentation and can demonstrate plausible deniability, one is safe from enforcement or liability. While this is not my area of expertise, I would urge the Commission to generally consider how incentives are structured, and always attempt to align incentives to produce the best possible outcomes with respect to system design, testing and stability. Safe Harbor is an excellent example of the misalignment of incentives that the Commission should be wary of.

That being said, if Safe Harbor provisions are included in the Rule, the Commission should be as specific as possible in establishing how to qualify for those Safe Harbor provisions. In addition, the Commission should make sure that such guidance ensures that SCI Entities are actively building and

improving upon safety systems, and not simply checking boxes and doing the minimal amount necessary to ensure compliance. This should mean that concrete actions are taken, recorded and demonstrable, i.e. capacity tests, independent testing for software and security problems, etc.

### **Questions on SCI Event Reporting**

Once again I simply want to stress that the Commission should be focused on transparency, and should therefore err on the side of overreporting rather than underreporting. This is not only critical to ensure that the Commission has a view into any problems at SCI Entities for regulatory purposes. As is the nature of complex systems and networks, local actors may not realize the importance of local problems, or the applicability of those problems / events to the market at-large. What may seem to be a minor, isolated, localized problem in one person's or group's eyes may have much broader consequences than they realize. It is the job of the regulator to have a broader perspective, and to make the final determination as to whether an event is important or not.

### **Conclusion**

Thank you for considering my comments on Regulation SCI. I applaud the Commission for continuing its efforts to reduce the frequency and impact of technology problems in equity markets. I would stress that any effort take into account the complexity of the world in which we are now operating, and the mistakes that have been made in the past. There must also be an equilibrium found when considering whether to foster competition versus when to place onerous and expensive rules on participants. I would simply state that in the past that balance has been skewed towards fostering competition, contributing to the overly complex system we have today. In the interests of complexity reduction, we should now err to the side of proper, effective rules with robust requirements to demonstrate compliance. I also believe it would be a grave mistake to not include broker-dealers and other participants with direct market access in the scope of this regulation, and would render the regulation far less effective.

I'll close with another quote from Sidney Dekker, and a reminder to not take a reductionist, componential approach to regulation of complex systems. We must embrace the complexity where we have no choice, and reduce it wherever possible.

“The growth of complexity in society has got ahead of our understanding of how complex systems work and fail. Our technologies have got ahead of our theories. Our theories are still fundamentally reductionist, componential and linear. Our technologies, however, are increasingly complex, emergent and non-linear. Or they get released into environments that make them complex, emergent and non-linear. If we keep seeing complex systems as simple systems – because of the dominant logic and inherited scientific-engineering language of Newton and Descartes – we will keep missing opportunities for better understanding of failure. We will keep missing opportunities to develop fairer responses to failure, and more effective interventions before failure.” - Sidney Dekker, [Drift Into Failure](#)

Respectfully submitted,  
David Lauer