Ms. Elizabeth M. Murphy
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,

I write on behalf the Consortium for IT Software Quality (CISQ) to provide comments regarding the SEC's proposed rulemaking on Regulation SCI (Systems Compliance and Integrity) that are in addition to comments provided in our letter marked as XXXX on the SEC's website. CISQ is a Special Interest Group of the Object Management Group (OMG), co-founded by the OMG and the Software Engineering Institute (SEI). These comments are provided as part of CISQ's mission to provide an industry voice for enhancing the quality of IT software. The comments in this letter are solely those of CISQ and should not be construed as representing the opinions of either of our founding organizations, OMG or SEI. Our previous letter provided comments regarding requests #60 - #79 and was submitted on July 8, 2013. This letter provides additional comments addressing requests #80 - #95.

Sincerely,

Dr. Bill Curtis

Director

Consortium for IT Software Quality (CISQ)

Specific Comments Regarding proposed Rule 1000(b)(1)

Note: The opinions responding to the numbered requests for comment will concentrate on the actual properties of the software code that cause problems such as outages, data corruption, slow recovery, etc. The properties of system integrity, resiliency, and availability will be referred to throughout these comments as 'reliability', since this term is used in international standards such as ISO/IEC 25010 and incorporates the properties of integrity, resiliency, and availability as sub-characteristics of reliability.

80. Would any of the Commission's proposed requirements under proposed Rule 1000(b)(1) create inappropriate barriers to entry for new entities seeking to register with the Commission as an SRO, ATS, or plan processor? Would any of the proposed requirements inappropriately limit the growth or expansion of entities currently registered with the Commission as an SRO, ATS, or plan processor?

Recommendation: All entities currently registered or seeking to register with the Commission as an SRO, ATS, or plan processor should be held to the same software quality practices that are proposed in Rule 1000(b)(1).

Discussion: The software quality practices in Rule 1000(b)(1) are standard practices in the software industry. They are particularly important in securities markets to protect institutions and investors. Any organization that could not or did not intend to implement these practices could inject unknown and potentially unacceptable levels of risk into automated market operations. In other industrial software domains, organizations have used advanced software reliability and quality to secure a superior market position that reduces or eliminates competition from organizations whose technology is less reliable or secure. This is a natural condition of competitive markets. If the SCI systems of current market participants do not provide reliable, secure service, then there is ample opportunity for the entry of new competitors who can enter with and sustain superior quality. Since higher quality software is cheaper to maintain and easier to enhance, any organization with the resources to develop the SCI systems needed to participate in these markets has the resources to compete effectively under the practices of Rule 1000(b)(1).

81. As noted above, the Commission proposes that policies and procedures would be deemed to be reasonably designed for purposes of proposed Rule 1000(b)(1) if they are consistent with current SCI industry standards.

Recommendation: Current industry standards in the SCI domain related to software reliability and security need to be strengthened beyond those in Table A which focus on development methods and practices and not on the properties of the actual software produced by these methods which can cause reliability or security problems. Thus we believe the deeming of “reasonably designed” needs to include criteria from additional standards.

Discussion: The most relevant standard for ensuring high quality software in Table A is NIST’s *Special Publication 800-64, Rev. 2*. The strength of this standard is its focus on the process for creating secure software. Processes related to other critical qualities such as reliability are not described. However, the methods and practices described in *800-64 rev. 2* can be adapted to cover other software quality characteristics critical to SCI systems such as reliability.

One caution in relying on a primarily process-based standard is that having state-of-the-art software development methods and supporting practices is a necessary, but not sufficient foundation for consistently producing reliable and secure software. Processes, practices, and methods alone are not sufficient because of the enormous influence developer knowledge and skill has on the development of knowledge-intense products such as software. Rigorous development practices do not eliminate gaps in developer knowledge and skill. This problem has been evident when organizations certified at Level 5, the pinnacle of CMMI capability, produced software with flaws that caused operational outages. Many times these problems were due to a large influx of young, inexperienced developers as the software organizations grew. Their learning curve could be shortened but not eliminated by high maturity development practices. Consequently, the structural quality of actual product must be evaluated to ensure it does not contain reliability or security-related flaws. Table A needs to be supplemented with a document that defines minimum standards for reliability and security that can be evaluated in the code. Such a standard would supplement the existing focus on process standards.

82. Do commenters believe that the publications listed in Table A represent publications that are suitable for purposes of proposed Rule 1000(b)(1)(ii) and that should be the “current SCI industry standards” for purposes of proposed Rule 1000(b)(1)(ii)?

Recommendation: The standards in Table A need to be supplemented with a standard that specifies violations of best software architecture and coding practices that can be measured to evaluate the reliability/resilience and security of SCI systems and compliance with the intent of Rule 1000(b)(1)(ii). This recommendation will be elaborated and discussed in our response to question 83.

83. Are there areas within one of the nine identified domains that these publications do not cover?

Recommendation: The list of standards in Table A should be expanded to include standards related to the structural quality characteristics of software directly relevant to SCI entity and market operations. Table A should include at a minimum the *CISQ Specifications for Automated*

Quality Characteristic Measures: CISQ-TR-2012-01 which enumerates specific structural flaws related to system reliability and security that should be eliminated for an SCI system to be deemed reliable and secure.

Discussion: The standards referenced in Table A are not sufficient of themselves to support compliance with Rule 1000(b)(1) in the area of software reliability and security because they do not provide guidance on the engineering or structural properties the software must possess to ensure the reliable and secure performance in operation. We strongly recommend that the *CISQ Specifications for Automated Quality Characteristic Measures: CISQ-TR-2012-01* be included in Table A since no other comparable standard for the actual quality characteristics of software controlling reliability and security is referenced. The Consortium for IT Software Quality (CISQ) is an industry consortium co-founded by the Software Engineering Institute at Carnegie Mellon University and the Object Management Group (a software industry standards organization) that operates as a special interest group of OMG. CISQ's initial objective was to define measures of software characteristics that could be measured from the source code of systems, since international standards were failing to provide measures at this level.

The CISQ standard is consistent with the definitions of both reliability and security in the relevant ISO software product quality standards, ISO/IEC 25010 and ISO/IEC 25023. While these international standards provided the conceptual foundation and high level guidance for the CISQ Quality Characteristic measures, they did not define these characteristics at the level of measureable attributes in the software code. The CISQ standard defines specific flaws that should not be present in software if it is to be deemed reliable and secure.

The CISQ standard defines measures of reliability and security by counting violations of architectural and coding best practices that are known to have caused outages or allowed unauthorized access to systems. For instance, the CISQ measure for security is based on the top 25 security weaknesses in software listed in the Common Weakness Enumeration (CWE), a publicly available repository of over 800 weaknesses in software architecture or coding that have been exploited to gain unauthorized access. The CWE is maintained by Mitre Corporation with support from the Department of Homeland Security, and was developed with concerted effort from the software assurance community to catalogue known security weaknesses. This standard will provide a strong supplement in Table A for ensuring that SCI systems are compliant with best software engineering practices for the architecture and coding of software.

Table A could also reference the widely adopted Capability Maturity Model Integration CMMI) from the Software Engineering Institute at Carnegie Mellon University, a Federally Funded Research and Development Center (FFRDC) sponsored by the US DoD, since it is the most widely adopted process standard for guiding the adoption of rigorous software development practices.

85. The Commission seeks comment on whether commenters believe that the identified publications, and the industry standards within, are adequate in terms of the detail, specificity and scope.

Recommendation: NIST Special Publication 800-64, Rev. 2 and any derivative standard to cover other software qualities such as reliability should be reviewed and if necessary revised by a panel of industry practitioners and technical experts to balance the requirement for rigor with the amount of practices and documentation specified in the standard.

Discussion: A caution in using process-based standards is to establish the required level of professional discipline without instituting bureaucracy. Standards such as *800-64, Rev. 2* have a tendency to require too many practices and an excessive documentation. For instance, there is evidence that CMMI's use as a certification standard is in decline because of the amount of documentation that must be generated and the cost of compliance appraisals. Several DoD software standards have been revised or replaced because of the same problem. Lean thinking must prevail in designing or revising such standards to ensure that they contain the minimally necessary methods and practices to achieve the desired result. This balance is best achieved when industry practitioners and technical experts collaborate to achieve and effective but not overly burdensome standard. Support for *800-64, Rev. 2* will decline if it proves too burdensome in compliance without a compensating return in additional reliability and security in operation.

86. Do commenters agree with the Commission's proposed policies and procedures approach to the requirements of proposed Rule 1000(b)(1)?

Recommendation: Policies and procedures must be supplemented with analysis of the software in SCI systems in order to demonstrate an SCI system is capable of providing the "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."

Discussion: Having strong policies and procedures is important to producing reliable, secure software. However, as has been described in answers to earlier questions, they are not enough. Outages, data corruption, unauthorized intrusions are the result of weaknesses in the software. Even when complying with "industry standard policies and procedures" it is possible to create software with flaws that are responsible for unreliable or insecure operations. SEC must demand evidence that these flaws have been identified and are being systematically eliminated from SCI systems.

87. Do commenters agree or disagree with the Commission's proposed criteria to evaluate publications suitable for inclusion on Table A as an SCI industry standard and to update such list? Do commenters agree with the proposed criteria that identified publications should be: (i) comprised of information technology practices that are widely available for free to information technology professionals in the financial sector; and (ii) issued by an authoritative body that is a U.S. governmental entity or agency, association of U.S. governmental entities or agencies, or widely recognized organization?

Discussion: SEC should only include standards in Table A that have been created through by agencies such as NIST or through recognized professional organizations such as the International Organization for Standards (ISO), the Object Management Group (OMG) and its special interest groups, the Institute of Electrical and Electronics Engineers (IEEE), the Open Group, and the Software Engineering Institute (SEI). These organizations have open processes for gathering wide industry input and updating standards on a periodic basis. Open rather than proprietary standards allow competitive ecosystems to develop that support the deployment and compliance to these standards with technology and services.

90. Do commenters believe the potential additional time SCI SROs allocate to this process would result in fewer SCI events by helping to ensure that SCI SROs properly implement systems changes?

Discussion: The analysis of SCI systems against a public standard describing the properties of reliable, secure software coupled with adequate remediation processes reduces the number of SCI events by eliminating their causes from SCI systems. The cost of recent outages in SCI systems easily justifies the additional effort in quality assurance. However, empirical evidence from software industry improvement programs demonstrates that the additional time added into quality assurance is more than compensated for by a reduction in rework to produce ROIs of 5:1 or greater.

95. Do commenters believe it would be feasible to establish industry standards through means other than identification through Table A? For example, should SCI entities take the lead in developing such standards?

Recommendation: SCI entities should consider tailoring a set of standards from professional standards organizations for use in SCI applications.

Discussion: The most effective way to create standards designed for the specific conditions of an industry segment is to begin with existing open standards from professional standards organizations and tailor them for industry segment use. These tailored standards may also be combined where sensible into an amalgamated standard. This approach shortens the time to establish a standard, builds in industry-wide learning and best practices, and ensures that critical practices are not overlooked.