**Securities and Exchange Commission**

**Staff Guidance on Current SCI Industry Standards**

**November 19, 2014**

The statements in this staff guidance were prepared by and represent the views of the staff. They are not rules, regulations, or statements of the Securities and Exchange Commission ("Commission"). Further, the Commission has neither approved nor disapproved this staff guidance.

**For Further Information Contact:** David Garcia, Special Counsel, at (202) 551-5681, Division of Trading and Markets, Securities and Exchange Commission, 100 F Street, NE, Washington DC 20549

## I. Regulation Systems Compliance and Integrity

On November 19, 2014, the Commission adopted Regulation Systems Compliance and Integrity, 17 CFR 242.1000-1007 ("Regulation SCI") under the Securities Exchange Act of 1934 ("Exchange Act").[1] Regulation SCI applies to certain self-regulatory organizations (including registered clearing agencies), alternative trading systems, plan processors, and exempt clearing agencies (collectively, "SCI entities"). Regulation SCI requires SCI entities to, among other things, establish, maintain and enforce 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 operate in a manner that complies with the Exchange Act. In the SCI Adopting Release, the Commission stated that it believes that the adoption of, and compliance by SCI entities with, Regulation SCI will advance the goals of the national market system by enhancing the capacity, integrity, resiliency, availability, and security of the automated systems of entities important to the functioning of the U.S. securities markets, as well as reinforce the requirement

[1] Securities Exchange Act Release No. 34-73639 (November 19, 2014) ("SCI Adopting Release"), available at: www.sec.gov.

that such systems operate in compliance with the Exchange Act and rules and regulations thereunder, thus strengthening the infrastructure of the U.S. securities markets and improving its resilience when technological issues arise.[2]

## II. Rule 1001(a) and the Role of Staff Guidance

Rule 1001(a)(1) of Regulation SCI requires each SCI entity to establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its SCI systems and, for purposes of security standards, indirect SCI 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. Rule 1001(a)(2) specifies that such policies and procedures are required to include, at a minimum: (i) the establishment of reasonable current and future technology infrastructure capacity planning estimates; (ii) periodic capacity stress tests of such systems to determine their ability to process transactions in an accurate, timely, and efficient manner; (iii) a program to review and keep current systems development and testing methodology for such systems; (iv) regular reviews and testing, as applicable, of such systems, including backup systems, to identify vulnerabilities pertaining to internal and external threats, physical hazards, and natural or manmade disasters; (v) business continuity and disaster recovery plans that include maintaining backup and recovery capabilities sufficiently resilient and geographically diverse and that are reasonably designed to achieve next business day resumption of trading and two-hour resumption of critical SCI systems following a wide-scale disruption; (vi) standards that result in such systems being designed, developed, tested, maintained, operated, and surveilled in a manner that facilitates the successful collection, processing, and dissemination of market data; and (vii) monitoring of such systems to identify

[2] See SCI Adopting Release at pages 18-19.

potential SCI events. Rule 1001(a)(3) requires each SCI entity to periodically review the effectiveness of the policies and procedures required by Rule 1001(a), and take prompt action to remedy deficiencies in such policies and procedures. Rule 1001(a)(4) states that for purposes of Rule 1000(a) an SCI entity's policies and procedures shall be deemed to be reasonably designed if they are consistent with current SCI industry standards, which are required to be comprised of information technology practices that are widely available to information technology professionals in the financial sector and 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, although compliance with current SCI industry standards is not the exclusive means to comply with the requirements of Rule 1001(a).

When the Commission proposed Regulation SCI [3] it set forth an example of a set of technology publications that the Commission preliminarily believed were appropriate to be referred to as "current SCI industry standards" because they met certain proposed criteria.[4] As described in more detail in the SCI Adopting Release, in response to comment, the Commission modified the proposed criteria for "current SCI industry standards." Specifically, the Commission eliminated the proposed requirement that information technology practices be

---

[3] Securities Exchange Act Release No. 69077 (March 8, 2013), 78 FR 18083, 18108-18111 (March 25, 2013) ("SCI Proposal").

[4] See SCI Proposal, 78 FR at 18111 (proposed Table A). Proposed Rule 1000(b)(1)(ii) stated that an SCI entity's policies and procedures would be deemed to be reasonably designed if they were consistent with "current SCI industry standards." As proposed, "current SCI industry standards" were required to be: (A) comprised of information technology practices that are widely available for free to information technology professionals in the financial sector; and (B) 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. See SCI Proposal, 78 FR at 18111. The proposed rule further stated that "compliance with such current SCI industry standards…shall not be the exclusive means to comply with the requirements of paragraph (b)(1)." See SCI Proposal, 78 FR at 18109.

available "for free." Therefore, as adopted, Rule 1001(a)(4) provides that an SCI entity's policies and procedures shall be deemed to be reasonably designed if they are consistent with current SCI industry standards, which are required to be comprised of information technology practices that are widely available to information technology professionals in the financial sector and 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.[5]

Further, in the SCI Adopting Release, the Commission stated that the staff should issue guidance to assist SCI entities in developing policies and procedures consistent with "current SCI industry standards."[6] The Commission explained that guidance issued by the Commission staff would, in its view, have the advantage of easier updating and allow for an emerging consensus on standards more focused on the securities industry. The Commission also stated that staff guidance should assist SCI entities in developing policies and procedures consistent with "current SCI industry standards" in a manner that is consistent with the Commission's response to comments received on proposed Table A, and periodically update such guidance as appropriate.[7] Accordingly, this Staff Guidance on current SCI industry standards ("SCI Staff Guidance") is issued to assist SCI entities on developing policies and procedures "consistent with current SCI industry standards."[8]

---

5 See SCI Adopting Release at page 183.

6 See SCI Adopting Release at page 187.

7 See SCI Adopting Release at page 187.

8 See Rule 1001(a)(4) of Regulation SCI.

## III. Staff Guidance on Current SCI Industry Standards

The staff guidance lists examples of publications describing processes, guidelines, frameworks, or standards an SCI entity could look to in developing reasonable policies and procedures to comply with Rule 1001(a) of Regulation SCI. These examples are not strictly a list of standards. On the table below, the staff provides a list of publications that the staff believes are appropriate for the specified domains to describe processes, guidelines, frameworks, or standards that may be used by SCI entities in developing their policies and procedures under Rule 1001(a) of Regulation SCI. The publications below cover nine inspection areas, or "domains," relevant to an SCI entity's systems capacity, integrity, resiliency, availability, and security: application controls; capacity planning; computer operations and production environment controls; contingency planning; information security and networking; audit; outsourcing; physical security; and systems development methodology. These publications are issued by the National Institute of Standards and Technology ("NIST"); Federal Financial Institutions Examination Council ("FFIEC"); financial regulatory agencies including the Commission; the Institute of Internal Auditors, and the Security Benchmarks division of the Center for Internet Security. In the staff's view, these publications satisfy the criteria for current SCI industry standards in Rule 1001(a)(4) of Regulation SCI: i.e., they are information technology practices that are widely available to information technology professionals in the financial sector and 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.[9] In

[9] In particular, the staff notes that NIST, which has published many of the documents contained in this SCI Staff Guidance, is a widely-recognized professional standards organization, and that NIST routinely collaborates with other widely-recognized

addition, the staff believes the publications identified are general and flexible enough to be compatible with many widely-recognized technology standards that SCI entities currently use.[10] These publications are identified as guidance for an SCI entity in developing reasonably designed policies and procedures pursuant to Rule 1001(a) of Regulation SCI.

**Staff Guidance on Current SCI Industry Standards**

| Domain | Publications |
|---|---|
| **Application Controls** | NIST Security and Privacy Controls for Federal Information Systems and Organizations (Special Publication 800-53 Rev. 4), available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. |
| **Capacity Planning** | FFIEC, Operations IT Examination Handbook (July 2004), available at: http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_Operations.pdf. |

standards organizations to develop its frameworks. The publications identified at this time have the additional benefit of being high-level documents focused on process that are routinely updated, technology neutral and flexible enough to provide a framework and guidance for rapidly evolving technology.

10 In particular, the staff notes that NIST 800-53 Rev. 4 maps to ISO/IEC 270001 and understands that there are documents and tools available to SCI entities that would likewise assist them in mapping the NIST 800-53 Rev. 4 framework to other technology standards issued by widely recognized standards organizations. See NIST 800-53 Rev. 4, Appendix H, stating that: "The mapping tables in this appendix provide organizations with a general indication of security control coverage with respect to ISO/IEC 27001, Information technology–Security techniques–Information security management systems–Requirements113 and ISO/IEC 15408, Information technology—Security techniques—Evaluation criteria for IT security." Therefore, if an SCI entity currently uses the ISO/IEC 270001 and COBIT frameworks in developing its policies and procedures, because NIST 800-53 Rev. 4 maps to ISO/IEC 270001 and COBIT, for example, it would not be inconsistent with the staff guidance for an SCI entity to continue to use the ISO/IEC 270001 and COBIT frameworks in developing its policies and procedures to meet the requirements of Rule 1001(a).

| | |
|---|---|
| **Computer Operations and Production Environment Controls** | NIST Security and Privacy Controls for Federal Information Systems and Organizations (Special Publication 800-53 Rev. 4), available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. |
| **Contingency Planning (BCP)** | NIST Contingency Planning Guide for Federal Information Systems (Special Publication 800-34 Rev. 1), available at: http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.<br><br>2003 Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, Securities Exchange Act Release No. 47638 (April 8, 2003), 68 FR 17809 (April 11, 2003) ("2003 Interagency White Paper"), available at: http://www.sec.gov/news/studies/34-47638.htm.<br><br>2003 Policy Statement on Business Continuity Planning for Trading Markets, Securities Exchange Act Release No. 48545 (September 25, 2003), 68 FR 56656 (October 1, 2003) ("2003 BCP Policy Statement"), available at: http://www.sec.gov/rules/policy/34-48545.htm. |
| **Information Security and Networking** | NIST Security and Privacy Controls for Federal Information Systems and Organizations (Special Publication 800-53 Rev. 4), available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.<br><br>NIST Guidelines on Security and Privacy in Public Cloud Computing (Special Publication 800-144), available at: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.<br><br>The Center for Internet Security Configuration Benchmarks, available at: http://benchmarks.cisecurity.org/en-us/?route=downloads.benchmarks.<br><br>NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.0, available at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf. |

| | |
|---|---|
| **Audit** | FFIEC, Audit IT Examination Handbook (August 2003), available at: http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_Audit.pdf.<br><br>IIA, The Role of Internal Auditing in Enterprise-wide Risk Management, available at: https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Role%20of%20Internal%20Auditing%20in%20Enterprise%20Risk%20Management.pdf and https://na.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx. |
| **Outsourcing** | FFIEC, Outsourcing Technology Services IT Examination Handbook (June 2004), available at: http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_OutsourcingTechnologyServices.pdf. |
| **Physical Security** | NIST Security and Privacy Controls for Federal Information Systems and Organizations (Special Publication 800-53 Rev. 4), available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. |
| **Systems Development Methodology** | NIST Security and Privacy Controls for Federal Information Systems and Organizations (Special Publication 800-53 Rev. 4), available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. |

For the domains of application controls; computer operations and production environment controls; and physical security, the staff has included the NIST 800-53 Rev. 4 framework in its final form. The staff believes NIST 800-53 Rev. 4 is compatible with many of the publications that commenters on the SCI Proposal identified as potential alternatives for inclusion on proposed Table A, including ISO 27000[11] and COBIT,[12] because it includes

[11] ISO 27000 is issued by the International Organization for Standardization, a non-governmental that develops and publishes international standards.

mapping tables for international security standard ISO/IEC 15408 (Common Criteria), and also because the security and privacy controls in NIST 800-53 Rev. 4 have been designed to be largely policy/technology-neutral to facilitate flexibility in implementation.[13] The staff also understands that mapping tables for NIST 800-53 Rev. 4 to ISO 27000, COBIT, and other technology standards are available.[14]

The staff has likewise identified NIST 800-53 Rev. 4 as a reference document in the systems development methodology domain. Although the Commission had included NIST Security Considerations in the System Development Life Cycle (Special Publication 800-64 Rev. 2) as a reference document on Table A in the SCI Proposal, consistent with the Commission's response to comments on this publication, the staff is instead identifying NIST 800-53 Rev. 4 for the systems development methodology domain. The staff believes NIST 800-53 Rev. 4 is more flexible than Special Publication 800-64 Rev. 2, and therefore more compatible for use with a variety of systems development methodologies employed by SCI entities.[15]

---

12 COBIT (formerly known as Control Objectives for Information and related Technology) is an enterprise information technology governance framework developed by ISACA (formerly known as the Information Systems Audit and Control Association).

13 See, e.g., http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf at 3.

14 See, e.g., Shared Assessments Program Industry Relevance Document (Mapping of AUP and SIG v5.0 to NIST SP 800-53), available from: www.sharedassessments.org. Further, the staff understands that mapping or referencing between other technology standards is available. For example, the NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.0, (February 2014), which is included in this SCI Staff Guidance, references industry standards including ISO 27000 and COBIT, and other publications. As a further example, with regard to the SANS 20 Critical Security Controls, SANS states that the "actions defined by the Controls are demonstrably a subset of the comprehensive catalog defined by the National Institute of Standards and Technology (NIST) SP 800-53." See http://www.sans.org/critical-security-controls.

15 Specifically, the staff understands that NIST 800-53 Rev. 4, unlike NIST 800-64 Rev. 2, does not favor one particular development method over another.

In the information security and networking domain, the staff believes that the NIST 800-53 Rev. 4, NIST Guidelines on Security and Privacy in Public Cloud Computing (Special Publication 800-144), and The Center for Internet Security Configuration Benchmarks are relevant reference publications. In addition, the staff has identified the NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 (February 2014) as a reference document in the information security and networking domain. Although the NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 (February 2014) was not referenced in the SCI Proposal, the staff notes that several panelists from the Cybersecurity Roundtable organized by the Commission[16] commented on the utility of it as a methodology for helping entities to address cybersecurity risk.[17] The staff also notes that the NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 (February 2014) references specific COBIT controls, and that COBIT was favored as an appropriate standard for inclusion on proposed Table A by several commenters to the SCI Proposal.[18]

In the contingency planning domain, the staff has identified the NIST Contingency Planning Guide for Federal Information Systems (Special Publication 800-34 Rev. 1), the 2003 Interagency White Paper and the 2003 BCP Policy Statement as relevant reference documents. The staff believes the 2003 Interagency White Paper and the 2003 BCP Policy Statement remain

---

16 See Securities Exchange Act Release No. 71742 (March 19, 2014), 79 FR 16071 (March 24, 2014) (File No. 4-673). A webcast of the Cybersecurity Roundtable is available at: http://www.sec.gov/news/otherwebcasts/2014/cybersecurity-roundtable-032614.shtml.

17 See http://www.nist.gov/itl/upload/alternative-view-framework-core-021214.pdf.

18 See SCI Adopting Release at page 189, note 584 and accompanying text.

relevant following the adoption of Regulation SCI.[19] In addition, the staff notes that the 2003 Interagency White Paper, in particular, identifies sound practices jointly developed by the Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, and the Commission, and also is relevant beyond the context of the securities markets.

The staff believes that FFIEC, Audit IT Examination Handbook (August 2003) and IIA, The Role of Internal Auditing in Enterprise-wide Risk Management are appropriate in the audit domain; that FFIEC, Operations IT Examination Handbook (July 2004) is an appropriate reference document in the capacity planning domain; and that FFIEC, Outsourcing Technology Services IT Examination Handbook (June 2004) are appropriate reference documents in the outsourcing domain.

Each listed publication in this SCI Staff Guidance is identified with specificity and includes the particular publication's date, volume number, and/or publication number, as the case may be. Thus, for SCI entities that establish their policies and procedures in reliance on the guidance provided by these listed publications, the listed publications set forth will be the relevant publications until such time as this list is updated by the staff.

Rule 1001(a)(4) of Regulation SCI explicitly provides that compliance with current SCI industry standards (i.e., including those publications listed here) is not the exclusive method of compliance with Rule 1001(a). Therefore, it may be appropriate for an SCI entity to choose to adhere to a standard or guideline in a given domain or subcategory thereof that is different from those contained in the publications identified in this SCI Staff Guidance.

---

[19] See SCI Adopting Release at pages 163-171 (discussing the Commission's adoption in Rule 1001(a)(2)(v) of concrete recovery goals that the policies and procedures must be reasonably designed to achieve, rather than hard and fast recovery deadlines).